ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Оцінка вразливостей пристроїв інтернету речей і пропозиція рішень безпеки»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Артем ХИТРІН
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД- 41
Артем ХИТРІН
Ім'я, ПРІЗВИЩЕ

Керівник: Юлія КАГРАМАНОВА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Хитріну Артему Олексійовичу

(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Оцінка вразливостей пристроїв інтернету речей і пропозиція рішень безпеки
керівник кваліфікаційної роботи Юлія КАГРАМАНОВА
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2. Принцип функціонування «розумного будинку».
3. Основні принципи гейміфікації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Кібербезпека пристроїв IOT. Визначення та теорія
2. Інструменти та прийоми забеспечення безпеки IOT
3. Оцінка вразливостей камери стеження за допомогою спеціалізованих інструментів

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	27.02-05.03.2024	
2	Обгрунтування актуальності роботи	06.03-11.03.2024	
3	Аналіз основних прийомів забеспечення безпеки	12.03-27.03.2024	
4	Інструменти та прийоми забеспечення безпеки IOT	28.03-10.04.2024	
5	Оцінка вразливостей камери стеження за допомогою спеціалізованих інструментів	11.04-15.05.2024	
7	Оформлення роботи: вступ, висновки, реферат	16.05-22.05.2024	
8	Розробка демонстраційних матеріалів	23.05-24.05.2024	

Здобувач(ка) вищої освіти _____ Артем ХИТРІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юлія КАГРАМАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавр: 55 сторінки, 29 рисунка та 25 джерел.

Мета роботи – Оцінка вразливостей пристроїв інтернету речей і надання рекомендацій з безпеки інформації за рахунок дослідження конкретного IOT девайсу.

Об'єкт дослідження- камери стеження.

Предмет дослідження – вразливості пристроїв інтернету речей.

Короткий зміст роботи: У роботі проаналізовано можливості оцінки безпеки і проведена спроба взлому пристоїв інтернету речей, на прикладі камери стеження. Використовуючи спеціалізовані інструменти кібербезпеи досліджено вразливості камер, та надані рекомендації з підвищення безпеки.

З камери було запозичено конфіденційні данні та використані для входу в облікові записи адміністраторів. Було використано вхідні дані для підбору пароля, використовував словникову атаку з використанням інструменту злому паролів JtR. Використав програмне забезпечення "Stealer", що призвело до вилучення файлу бази даних віддалених користувачів з усіма обліковими даними. Це підтверджує необхідність ретельної оцінки вразливостей, розробки та впровадження ефективних заходів безпеки у всіх IOT пристроях.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, ЗАХИСТ ПРИСТРОЇВ IOT, ОЦІНКА ВРАЗЛИВОСТЕЙ, ІНСТРУМЕНТИ ТЕСТУВАННЯ, ЗАХОДИ МЕРЕЖЕВОЇ БЕЗПЕКИ, ПЛАН ПІДВИЩЕННЯ БЕЗПЕКИ.

ABSTRACT

The textual part of the qualifying work for the bachelor's degree: 55 pages, 29 figures and 25 sources.

The purpose of the work is to assess the vulnerabilities of Internet of Things devices and provide recommendations on information security through the study of a specific IOT device.
The object of research is surveillance cameras.
The subject of the study is the vulnerability of Internet of Things devices.

Brief content of the work: The work analyzed the possibilities of security assessment and conducted an attempt to hack the Internet of Things, using the example of a surveillance camera. Using specialized cyber security tools, the vulnerabilities of the cameras were investigated, and recommendations for improving security were provided.

Sensitive data was borrowed from the camera and used to log into administrator accounts. Input was used to guess the password, used a dictionary attack using the JtR password cracking tool. Used "Stealer" software, which led to the extraction of the remote user database file with all credentials. This confirms the need for thorough vulnerability assessment, development and implementation of effective security measures in all IOT devices.

KEY WORDS: CYBER SECURITY, SECURITY OF IOT DEVICES, VULNERABILITY ASSESSMENT, TESTING TOOLS, NETWORK SECURITY MEASURES, SECURITY ENHANCEMENT PLAN.

РЕЦЕНЗІЯ

Зміст

ВСТУП

Зростаюче використання пристроїв IoT призвело до зростання ризиків з точки зору кібербезпеки. Робота присвячена аналізу вразливостей пристроїв IoT та розробці рекомендацій щодо підвищення інформаційної безпеки в мережі Інтернет.

У майбутньому розвиток Інтернету речей змінить можливості, які ми використовуємо та взаємодіємо з навколишнім середовищем. Від побутових пристроїв, таких як розумні годинники та електронні пристрої, до промислових систем керування та повністю автоматизованих пристроїв, IoT став необхідною частиною нашого сучасного життя та виробничих процесів.

Однак із зростанням використання IoT постають нові виклики з точки зору кібербезпеки. Багато пристроїв IoT мають обмежені ресурси, обслуговуються застарілим програмним забезпеченням і недостатньо захищені від кіберзлочинців. Це створює серйозну загрозу для конфіденційності, цілісності та доступності інформації, яка обробляється та передається цими пристроями.

Розгортання пристроїв Інтернету речей (IoT) через мережі створює значні робочі проблеми та проблеми безпеки, такі як виявлення та пом’якшення вразливостей кібербезпеки. Нещодавні дослідження показали, що загрози безпеці зберігаються в області Інтернету речей, і підкреслили необхідність звернути увагу на зростаючий обсяг досліджень уразливостей.

Зі збільшенням кількості взаємопов’язаних пристроїв і впровадження інноваційних технологій IoT, виявлення вразливостей і керування ними стає все складнішим.

Щоб розробити масштабований метод, який може йти в ногу з передовими технологіями оцінки вразливості, необхідно визначити найбільш уразливі типи пристроїв IoT і зрозуміти конкретні вразливості. Це дослідження має на меті підтвердити рівень ризику та важливість безпеки гаджетів інтернету речей за допомогою сучасних інструментів оцінки та баз даних, а також загальних вразливостей і вразливостей (CVE).

Важливість цієї дипломної роботи полягає в дослідженні постійних проблем безпеки в сфері Інтернету речей, підкреслюється необхідність розгляду зростаючої кількості доказів, що стосуються вразливостей кібербезпеки. Це дослідження спрямоване на виявлення сприйнятливих типів пристроїв IoT і вразливостей, пов'язаних із споживчими пристроями IoT, шляхом застосування передових інструментів і методів оцінки вразливостей.

Метою даної дипломної роботи є аналіз вразливостей пристроїв IoT та розробка рекомендацій щодо підвищення інформаційної безпеки в мережі IoT.

Для виконання завдання розглянуті перспективи розвитку концепції IoT, включаючи технології та стандарти для комутації та конвергенції інфраструктури Інтернету речей. Також досліджено різні варіанти підключення IoT до існуючих мереж та розглянуто архітектуру Інтернету речей.

Далі надано огляд основних проблем та загроз інформаційній безпеці Інтернету речей у мережах. Також наведено відповідні методи захисту інформаційної безпеки для подолання цих проблем та запобігання загрозам.

Потім представлено дослідження пристроїв Інтернету речей, використовуючи відомі вразливості інформаційної безпеки та особливості нормативних вимог. Запропоновано методи сканування пристроїв IoT, використовуючи сканер Network Mapper (Nmap) і пошукову систему Shodan. Проведено аналіз результатів сканування портів та запущених серверних служб з подальшим формуванням висновків. Використовуючи сканування, було проведено дослідження відповідних сервісів з використанням загальновідомих вразливостей.

Також проведено якісну та кількісну оцінку ризиків. Якісна оцінка дозволила визначити перелік пріоритетних загроз, які потім були піддані кількісній оцінції. У процесі кількісної оцінки визначено вплив цих пріоритетних загроз на цільові показники проекту з урахуванням ймовірності їх виникнення.

Крім того, була показана економічна ефективність запропонованих методів безпеки щодо зниження ризиків. Це значно знизило кінцевий ризик і покращило рівень безпеки для споживачів IoT.

Як я вже зазначив, порушення безпеки мережі стають все більш поширеними та дорогими. Необхідно знати потенційні вразливості безпеки в мережевій інфраструктурі.

Організації повинні захищати свої мережі та програми від будь-яких хакерських загроз або кібератак. Для цього окремі організації можуть запроваджувати засоби контролю безпеки додатків і мережі. І одним із найважливіших заходів/практик безпеки мережі є виконання поглибленої оцінки вразливості мережі.

Проведення оцінки вразливості мережі допомагає організаціям виявити будь-які слабкі місця у своїй системі раніше, ніж це зроблять зловмисники. Він також надає детальну інформацію про те, як пріоритетно усунути ці вразливості.

1 АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Поняття Інтернету речей

Інтернет речей є однією з найбільш універсальних технологій, які існують сьогодні. Поширення Інтернету, постійно зростаюча пропускна здатність і різноманітність розумних пристроїв сприяють вибуховому зростанню Інтернету речей у всьому світі.

Темпи зростання популярності Інтернету речей будуть тільки продовжувати збільшуватися. До 2025 року загальна кількість розумних пристроїв досягне 32 млрд.

У такій мережі немає користувачів, служб і баз даних, це окремі сегменти, об'єднані через Інтернет пристрої, де не має людського впливу.

IoT – це дуже зручний і корисний набір технологій, який значно спрощує як наше повсякденне життя, так і роботу підприємств. Незважаючи на зростаючу поширеність і легкість використання пристроїв IoT, ці пристрої налічують ряд своїх проблем. А саме: різноманітні вразливості, які складно визначити і відсутність стандартизації. Мережі IoT – це комплекси, де людина з’являється рідко, відповідно, відстеженням нестандартних ситуацій та вірусів ніхто не займається.

1.2 Виклики та загрози, пов'язані з безпекою IoT

Злочинці можуть залишатися непоміченими дуже легко. Всі розумні гаджети IoT є вразливими точками проникнення в мережу будь-якого бізнесу та підприємства. Тому такі пристрої частіше за все використовують начальною точкою великих зломів.

У наш час найпоширеніший спосіб взлому є хакінг пристроїв співробітників компаній.

Крім того, розвиток штучного інтелекту та машинного навчання здійснив революцію в кібербезпеці, дозволивши виявляти загрози та реагувати на них у реальному часі. Сьогодні кібербезпека — це багатогранна дисципліна, яка охоплює не лише технології, але й людські фактори, політику та правила, що відображає потребу в цілісному та проактивному підході до захисту цифрових активів і конфіденційності у все більш взаємопов’язаному світі.

Безпека оТ є важливою через сприйнятливість пристроїв IoT і зростаюче використання апаратного забезпечення IoT. Багато пристроїв IoT залишаються незашифрованими та можуть діяти як шлюз для хакерів, де один зламаний пристрій може надати комусь доступ до всієї підключеної

мережі. Без належної практики безпеки Інтернету речей компанії можуть зіткнутися з новими загрозами, що надходять із кіберпростору.

1.3 Ідентифікація типових вразливостей IoT-пристроїв

Основні вразливості застосовувані хакерами:

– DDoS-атака: це по суті законне використання онлайн-сервісу, яке заходить занадто далеко. Наприклад, веб-сайт може обробляти певну кількість запитів за хвилину. Якщо це число перевищено, продуктивність веб-сайту погіршується або він може бути повністю недоступним. Це перевантаження може бути спричинене атакою або навіть законним використанням.

– Програмний експлойт: більшість кіберзлодіїв користуються поширеними вразливостями в програмах девайсу, за для здійснення атаки. Зазвичай розробники закривають виявлені «діри» в безпеці в оновленнях. Однак у повсякдений час оновлені версії програмного забезпечення не завантажуються на пристрій вчасно. Це робить їх уразливими до атак. Додаткова загроза полягає в тому, що частина компаній пристроїв не розповідають своїм користувачам про спарвжній стек технологій програмного забезпечення, мотивуючи це ринковими стимулами.

– Атака MITM (атака через людей): хакери можуть перехоплювати мережевий трафік (перебуваючи в середині лінії обміну інформації між пристроєм-відправником і пристроєм-одержувачем) і отримувати дані користувачів та засекречену інформацію, якою девайси обмінюються через часні інтернет мережі. Оскільки багато інтелектуальних девайсів у більшості випадків не зашифровані, хакерам не складно отримати несанкціонований доступ до системи.

– Фізичне втручання

– Автоматизація та штучний інтелект: технології ШІ вже використовуються в глобальному масштабі. Але автоматизація має недолік: потрібна лише одна програмна помилка або несправний алгоритм, щоб вивести з ладу всю мережу ШІ та інфраструктуру, за яку він відповідав.

– Атаки Bruteforce: компанії зазвичай не приділяють достатньої уваги безпеці паролів пристроїв Інтернету речей, це робить їх уразливими до потенційних атак грубої сили або bruteforce. Часто паролі пристроїв IoT залишаються незмінними після інсталяції використовуючи головний пароль (admin), що дозволяє зловмисникам легко їх підібрати.

– Перехоплення мікропрограм: за врахування того, що оновлення мікропрограми пристрою не було підписано криптографічно або програмним забезпеченням. Передається по незахищеному каналу зв’язку, це дозволяє

зловмисникам перехопити його та завантажити шкідливе програмне забезпечення на пристрій під виглядом оновлень.

Якщо компоненти мають вразливі місця, кіберзлочинці можуть скористатися ними, щоб отримати контроль над пристроєм.

1.4 Виявлення потенційних атак та їх наслідків

Далі описана ідентифікація типових вразливостей пристроїв IoT, виявлення потенційних атак та їх наслідків, а також оцінку ризиків для інформаційної безпеки.

Пристрої Інтернету речей (IoT) мають низку унікальних вразливостей, які створюють потенційні шляхи для кібератак. Щоб ефективно захистити мережу IoT, важливо розуміти вразливості та їхні можливі наслідки. У цьому розділі ми проаналізуємо типові вразливості пристроїв IoT та їх можливі наслідки.

– Слабкі паролі та аутентифікація:

Багато пристроїв IoT постачаються з паролями за замовчуванням, які легко зламати. Недостатня або відсутня автентифікація може призвести до несанкціонованого доступу до пристроїв і мережі.

– Застаріле програмне забезпечення:

Багато пристроїв IoT не мають механізмів автоматичного оновлення програмного забезпечення. Використовуючи застаріле програмне забезпечення, є ризик стати жертвою різноманітних вразливостей.

– Недостатній захист мережевого трафіку:

Багато пристроїв IoT передають дані відкрито без шифрування. Це може призвести до перехоплення конфіденційної інформації, такої як особисті дані користувачів або паролі.

– Відсутність механізмів безпеки віддаленого доступу:

До багатьох пристроїв IoT можна отримати віддалений доступ через Інтернет за допомогою IP-адресів без належних механізмів безпеки. Це може призвести до несанкціонованого керування пристроєм або витоку конфіденційної інформації.

– Використання відомих протоколів і портів:

Багато пристроїв IoT використовують добре відомі протоколи та порти, які можна легко використати для атак. Атаки на порти часто використовуються для витоку доступу до пристроїв.

– Фізична недоступність:

Багато пристроїв IoT знаходяться у віддалених або недоступних місцях, що робить їх уразливими для фізичних атак. Наприклад, зловмисник може отримати фізичний доступ до пристрою та встановити на нього зловмисне програмне забезпечення.

Розуміння цих вразливостей дозволить розробити ефективні стратегії захисту для пристроїв IoT і мережі в цілому.

Підсумуємо:

– Поняття Інтернету речей (IoT):

IoT - це мережа фізичних пристроїв, які обмінюються даними та взаємодіють один з одним через Інтернет. Ці пристрої можуть бути різних типів, від побутових пристроїв, таких як холодильники та домашні термостати, до промислових систем управління.

– Виклики та загрози, пов'язані з безпекою IoT:

Недостатня захищеність: багато IoT-пристроїв мають обмежені ресурси для захисту, що робить їх вразливими перед атаками.

Незахищена комунікація: відсутність або недостатня шифрування комунікацій може призвести до перехоплення або модифікації даних.

Недостатня оновлення програмного забезпечення: багато виробників не надають регулярні оновлення для своїх пристроїв, що робить їх вразливими перед новими загрозами.

Використання за замовчуванням: багато користувачів не змінюють стандартні паролі та налаштування, що робить їхні пристрої легкими мішенями для атак.

– Попередні дослідження в області безпеки IoT:

Дослідження в цій області виявили багато вразливостей та потенційних атак, таких як атаки з вимаганням викупу, атаки на відмову в обслуговуванні (DoS), а також атаки на перехоплення даних.

– Ідентифікація типових вразливостей IoT-пристроїв:

Недостатність автентифікації: брак або слабка автентифікація може дозволити зловмисникам доступ до пристрою.

Вразливості в програмному забезпеченні: помилки в програмному забезпеченні можуть бути використані для отримання несанкціонованого доступу.

Недостатня захищеність мережі: слабкість в захищеності мережі може дозволити зловмисникам перехоплювати та модифікувати дані.

– Виявлення потенційних атак та їх наслідків:

DoS атаки можуть призвести до відмови в роботі IoT-пристроїв, що може мати серйозні наслідки в залежності від контексту (наприклад, атака на медичний пристрій).

Атаки на перехоплення даних можуть призвести до розголошення конфіденційної інформації або порушення приватності користувача.

– Оцінка ризиків для безпеки інформації:

Оцінка ризиків повинна включати оцінку потенційних загроз, вразливостей та наслідків атак для конкретних IoT-пристроїв.

Важливо також враховувати контекст використання пристрою та його вплив на безпеку користувача та інформацію.

Загалом, аналіз вразливостей пристроїв IoT є невід'ємною частиною їхньої безпеки та вимагає системного підходу, що включає в себе ідентифікацію, оцінку та мінімізацію ризиків.

У наступних розділах розглянемо методи оцінки безпеки та рекомендації щодо підвищення безпеки систем IoT.

2 МЕТОДИ ОЦІНКИ БЕЗПЕКИ ІОТ-ПРИСТРОЇВ

Інтернет речей охоплює велику кількість підключених до мережі пристроїв, які обмінюються даними через Інтернет. Це явище стало можливим завдяки надійній пропускній здатності мережі, поширеним бездротовим з'єднанням і доступним комп'ютерним чіпам.

IoT спрощує комунікацію між різноманітними об'єктами, використовуючи розширені датчики та забезпечуючи зв'язок у реальному часі. Це дозволяє пристроям обробляти інформацію на місці без затримок.

Перевірка IoT включає аналіз функцій, які пристрої виконують, їх ефективність і захищеність від кіберзагроз. Також важливо оцінити зручність використання, враження користувача і можливість інтеграції з іншими системами.

Проте тестування програмного забезпечення для IoT все ще потребує удосконалення. Спеціалісти з кібербезпеки повинні зосередитися на тестуванні, спрямованому на потреби користувачів, та проактивно запобігати помилкам, а не просто виявляти їх. Інженерам з контролю якості слід брати участь як у операційних процесах, так і у процесах розробки.

Для забезпечення якості програмного забезпечення тестувальникам потрібні глибокі знання предметної області. Ті, хто не має досвіду у тестуванні вбудованих систем або апаратного забезпечення, повинні розвивати свої навички в цих областях, щоб ефективно вирішувати унікальні виклики, пов'язані з тестуванням IoT.

Тестування пристроїв IoT передбачає ефективне виконання всіх функцій кожного елемента, щоб гарантувати, що мережа IoT працює спільно і забезпечує очікувані результати.

Тестування для IoT є важливим для того, щоб визначити, чи відповідає програмне забезпечення IoT стандартам якості та очікуванням користувачів. Оскільки якість продукту залежить від цього, тестувальники мають уважно перевіряти програмне забезпечення, щоб швидко виявляти та усувати основні помилки.

У Інтернеті речей мережа взаємопов'язаних пристроїв співпрацює гармонійно. Тому навіть одну помилку в цих програмах може бути складно виявити. Ефективність усіх пристроїв залежить від якості кожної системи.

2.1 Сканування мережі на предмет вразливостей

Ціль тестування IoT відображається у наступних перевагах:

• Покращена взаємодія з користувачем: Гарантована працездатність пристроїв IoT сприяє поліпшенню взаємодії з користувачем, що збільшує задоволення від використання та користування ними.

• Підвищена безпека: Оскільки пристрої IoT опрацьовують конфіденційні дані, тестування допомагає виявити вразливі місця, забезпечуючи заходи безпеки та захист від хакерських атак та кіберзагроз.

• Зменшення вартості: Раннє тестування дозволяє виявити та виправити проблеми, уникнувши дорогих проблем у майбутньому, що зменшує ризик відкликання продукту або несправності його роботи.

• Підвищена продуктивність: Тестування виявляє проблеми з продуктивністю, такі як проблеми з підключенням або недостатній час автономної роботи, що дозволяє виробникам представляти пристрої, що відповідають вимогам та очікуванням.

• Краща сумісність: Тестування гарантує, що пристрої IoT від різних виробників можуть працювати разом без проблем, забезпечуючи безперервну взаємодію та сумісність пристроїв.

Для підвищення ефективності тестування та досягнення кращих результатів було розроблено різні інструменти та інфраструктури тестування, які забезпечують автоматизацію, зменшення витрат, скорочення часу виходу на ринок і покращення загальних процесів тестування.

У цьому розділі описано методи оцінки безпеки Інтернету речей, включаючи сканування мережі на наявність вразливостей, використання інструментів аналізу трафіку та тестування на проникнення.

Загалом методи оцінки безпеки пристроїв IoT є важливими для захисту від кіберзагроз, захисту конфіденційних даних, підтримки робочої цілісності та забезпечення відповідності нормативним вимогам.

Інвестуючи в надійні заходи безпеки, організації можуть зменшити ризики, зберегти довіру та забезпечити майбутнє послуг і програм із підтримкою Інтернету речей.

2.2 Використання інструментів аналізу трафіку

Оцінка безпеки пристроїв IoT є ключовим кроком у забезпеченні їх захисту від потенційних кіберзагроз. Для ефективного виявлення вразливостей і розробки стратегій захисту використовуються різні методи оцінки безпеки. Далі наведені основні методи оцінки безпеки пристроїв IoT.

Сканування мережевих вразливостей:

• Використання спеціалізованих програм для сканування мережі на наявність вразливостей в IoT-пристроях. Дозволяє виявити такі вразливості, як відкриті порти, застаріле програмне забезпечення та слабкі конфігурації безпеки.

Аналіз мережевого трафіку:

• Моніторинг і аналіз мережевого трафіку для виявлення незвичайної або підозрілої активності. Детальний аналіз може допомогти виявити атаки, спроби несанкціонованого доступу та інші загрози безпеці.

Тест на проникнення:

• Проведення контрольованих атак на мережу та пристрої з метою виявлення слабких місць та вразливостей. Цей метод дозволяє оцінити реальний рівень захисту мережі та пристроїв від кібератак.

Аудит безпеки програмного забезпечення:

• Проведення аудиту програмного забезпечення для виявлення вразливостей, помилок коду та потенційних ризиків безпеці. Цей метод дозволяє виявити проблеми безпеки на програмному рівні та розробити план усунення.

Оцінка фізичної безпеки:

• Аналізуйте фізичний доступ до пристроїв та інфраструктури Інтернету речей, щоб виявити потенційні загрози. Включає оцінку захисту пристроїв від фізичних атак і можливостей злому на основі їх розташування.

Тест на проникнення:

• Залучення профільних спеціалістів для проведення реальних атак на мережу та пристрої з метою виявлення вразливостей. Цей метод дозволяє імітувати реальні сценарії атак і оцінювати реакцію системи на них.

Використання цих методів оцінки дозволить визначити потенційні загрози та розробити ефективні заходи захисту для пристроїв IoT і мережі в цілому.

Проведення комплексного тестування IoT може призвести до створення надійних додатків, які відповідають очікуванням користувачів і нормативним вимогам. Однак тестування систем IoT зіткнеться з рядом проблем, серед яких:

– Складність і різноманітність: системи IoT складаються з різних пристроїв з унікальними вимогами та можливостями, що ускладнює розробку універсальної стратегії тестування.

– Тестування апаратного та програмного забезпечення: Тестування IoT потребує поєднання апаратного та програмного тестування, включаючи протоколи зв'язку та тестування мережі.

– Тестування в реальному середовищі: Розгортання пристроїв IoT в різних середовищах ускладнює точне відтворення реальних умов та прогнозування їхньої поведінки.

– Проблеми безпеки: Протоколи IoT, підключені до Інтернету, стають жертвами кібератак, тому перевірка безпеки має велике значення для захисту конфіденційних даних.

– Масштаб та обсяг: Велика кількість пристроїв IoT вимагає масштабованих рішень для ефективного тестування всіх пристроїв та забезпечення повного охоплення.

– Інтероперабельність: Пристрої IoT часто взаємодіють один з одним та з іншими системами, вимагаючи комплексного тестування сумісності та бездоганної інтеграції.

– Конфіденційність даних: Пристрої IoT збирають та передають особисті дані, що вимагає ретельного тестування для захисту конфіденційності користувачів та дотримання правил захисту даних.

Для розв'язання цих проблем потрібна системна стратегія тестування, що охоплює всі етапи розробки. Співпраця різноманітних тестувальників з різним рівнем кваліфікації може забезпечити повноцінне тестування всіх аспектів IoT систем. Крім того, використання різноманітних інструментів

тестування та автоматизація можуть підвищити продуктивність і точність тестування пристроїв IoT.

3 РЕКОМЕНДАЦІЇ З ПІДВИЩЕННЯ БЕЗПЕКИ IOT

У розділі наведено рекомендації щодо покращення безпеки IoT. Підвищення безпеки пристроїв Інтернету речей (IoT) вимагає комплексного підходу та впровадження різноманітних заходів. Ключові рекомендації щодо покращення безпеки Інтернету речей для зменшення кіберзагроз, захисту пристроїв і мережі:

- Регулярне встановлення оновлень програмного забезпечення
- Реалізація суворої аутентифікації та авторизації
- Використання заходів безпеки мережі
- Навчання користувачів правилам кібербезпеки
- Моніторинг та аналіз діяльності
- Резервне копіювання даних
- Використання бездротових мереж із підтримкою шифрування

Ретельне впровадження заходів безпеки має вирішальне значення для забезпечення безпеки та конфіденційності користувачів у світі Інтернету речей. Основні компоненти систем Інтернету речей досить вразливі до атак зловмисників. Незалежно від масштабу та типу середовища, у якому вбудована система IoT, безпека має бути розглянута на етапі проектування, щоб покращити її інтеграцію.

Особливою проблемою для інженерів і фахівців з інформаційної безпеки є те, що через технологічний характер IoT неможливо встановити агента для перевірки на наявність інфекцій або вразливостей. Основні задачі команди захисту для забезпечення безпеки:

- Керування поверхнею атаки, слідкування за усіма гаджетами:

На час проектування безпеки IoT одним із головних завдань являє собою створення карти наявних IoT пристроїв у системі для їх звірки. Команда безпеки повинна володіти точною інформацією за кількістю задіяних пристроїв, та назву моделей виробників, номери продукції, версії програм та компонентів. Моніторинг, аналіз і звітність у лайв-режимі є критично необхідними в компаніях та підприємствах, для управління вразливостями Інтернету речей. Однак всебічно використовуючи розв’язання безпеки головних об’єктів мережі у більшості випадків користуються методом програмного агента, який не підходить для пристроїв Інтернету речей.

3.1 Безагентні методи для відслідковування поверхні атаки

Існують найсучасніші технології, а саме безагентні методи для відслідковування поверхні атаки. Ці можливості визначають оцінку ризиків у реальному часі шляхом постійного аналізу поведінки та справності всіх підключених пристроїв IoT. Деякі рішення в цьому відношенні навіть дозволяють попередньо когнітивно керувати поверхнею атаки, беручи до уваги ризики потенційних атак нульового дня.

Далі наведено інструменти безпеки дозволяють організаціям повною мірою скористатися перевагами технології IoT, одночасно усуваючи її головний недолік – відсутність безпеки.

– Поділ мережі на підмережі:

Це архітектурний проект мережі, який поділяє мережу на кілька сегментів (підмереж), кожен з яких функціонує як менша окрема мережа. Сегментація працює, контролюючи потік трафіку в мережі. Трафік можна обмежити в сегментах або на сегментах залежно від місця розташування, а також місця, де рух транспорту може, а де ні. Потік трафіку також може бути обмежений типом трафіку, джерелом і пунктом призначення.

– Застосування якісних паролів

Пристрої IoT часто мають стандартні або слабкі паролі, які легко зламати. Це залишає простір для атак грубої сили або ботів, які підбирають пароль. Вони можуть отримати несанкціонований доступ до пристрою, щоб дистанційно керувати ним або викрасти конфіденційні дані. Таким чином, зміна паролів є важливою для безпеки пристроїв IoT.

– Фізично захистити всі пристрої IoT

Фізична безпека пристроїв важлива, так-як злочинці мають можливість фізично втручатися в зовнішні пристрої, щоб отримати несанкціонований доступ або завантажити небезпечне програмне забезпечення в систему. Тому необхідно забезпечити надійне розташування пристрою.

– Своєчасне оновлення прошивки

Нові версії мікропрограми можуть виправити наявні вразливості пристрою. Отже систематичні апдейти значно підвищать спільну безпеку IoT. Однак оновлене програмне забезпечення треба досліджувати на наявність підробок, так-як шахраї у змозі використовувати вигляд оновлення для завантаження зловмисного програмного забезпечення на пристрій.

Атаки на інтернет мережі постійно адаптуються і змінюються. Отже треба бути в темі подій у кіберіндустрії та систематично оновлювати програмне забезпечення.

3.2 Використання заходів мережевої безпеки

Вбудовування безпеки в SDLC (Software Development Life Cycle)

Щоб реалізувати безпечніше майбутнє, знадобиться зміна парадигми. Створення майбутнього з більш безпечними пристроями IoT вимагає вбудови безпеки в життєвий цикл розробки програмного забезпечення (SDLC).

Життєвий цикл розробки програмного забезпечення (SDLC) відноситься до процесу, який використовується групами розробників програмного забезпечення для проектування, розробки, тестування та розгортання високоякісних програмних продуктів. Це структурований підхід, який окреслює різні етапи та дії, пов’язані зі створенням програмного забезпечення, від початкової концепції до її остаточного впровадження та обслуговування.

Ось короткий огляд кожного етапу SDLC і способів убудувати в нього безпеку:

– План:

Цей етап включає визначення вимог до того, що програмне забезпечення буде робити, а також оцінку витрат, планування, потреб у закупівлях і персоналу, необхідного для його впровадження.

Він також повинен містити компонент безпеки: моделювання загроз. Мета, яку іноді називають «думати як хакер», полягає в тому, щоб вийти за рамки стандартного списку відомих атак і визначити можливі загрози, які є унікальними для того, як побудована система або для чого вона призначена.

Ефективне моделювання загроз включає виділення активів, агентів загроз і елементів керування, щоб визначити, на які компоненти зловмисники, швидше за все, будуть спрямовані, а потім розробку заходів для усунення цих загроз.

Існує багато переваг моделювання загроз, але одна з найважливіших полягає в тому, що воно може заощадити час і гроші. Раннє виявлення потенційних проблем, ще до написання єдиного рядка коду, може виявити недоліки в дизайні, які традиційне тестування та перевірка коду можуть пропустити. Виправити або уникнути їх завчасно дешевше та швидше.

– Код:

Цей етап передбачає написання програмного коду для виконання вимог до дизайну. Інструменти статичного тестування безпеки додатків (SAST) допомагають розробникам знаходити та виправляти дефекти безпеки та якості під час написання коду. Найкращі у своєму класі інструменти виконують швидкий і поетапний аналіз у фоновому режимі, щоб мінімізувати збої. Розробники отримують результати в режимі реального часу, включаючи інформацію про CWE та вказівки щодо виправлення, безпосередньо в IDE.

– Розробка:

Сучасне програмне забезпечення рідко просто пишеться групою розробників. Він зібраний. Деякі компоненти є власністю, а інші – з комерційних бібліотек або бібліотек з відкритим кодом.

– Тестування:

Це вже окремий етап, коли команда безпеки досліджує програмне забезпечення на наявність вразливостей наприкінці SDLC. Тестування має бути всеохоплюючим, від моделювання загроз до початку кодування й аж до виробництва. Це вимагає кількох інструментів тестування, включаючи статичне, динамічне та інтерактивне тестування; фаз-тестування протягом розробки; аналіз складу програмного забезпечення (SCA) для пошуку вразливостей або конфліктів ліцензування з відкритим кодом. Перед розгортанням програмного забезпечення також потрібне тестування на проникнення (докладніше про це нижче).

Якщо з пристроями зв’язуються різні протоколи, Fuzz-тестування гарантує, що система загалом безпечна та надійна. Загальні протоколи включають Інтернет-протоколи, як-от IPv6, або протоколи короткого радіусу

дії, як-от Bluetooth, а нові протоколи, як-от Thread для використання з низьким енергоспоживанням і малою затримкою, набувають все більшого поширення.

3.3 Інструменти тестування кібербезпеки

Нарешті, тестування на проникнення використовує різноманітні інструменти тестування та ручні тести для пошуку та усунення критично важливих для бізнесу вразливостей у роботі веб-додатків і веб-служб без необхідності використання вихідного коду. Це «останній шанс» виявити та виправити значні вразливості, перш ніж оприлюднити ці програми та служби у всьому світі, де зловмисники шукатимуть способи зламати та використовувати їх.

Очевидно, набагато краще, щоб тестери виявляли дефекти раніше, ніж це зроблять загрозливі особи. Synopsys пропонує два рівні тестування пера на основі профілю ризику кожної перевіреної програми. Основний рівень включає автоматичне сканування та ручне тестування. Він зосереджений на дослідницькому аналізі ризиків (наприклад, антиавтоматизація, складна автентифікація). Стандартний рівень включає основні послуги, а також час і зусилля на тестування для вивчення бізнес-логіки, що охоплює атаки поза попередньо визначеним списком або ті, які, можливо, не розглядалися інакше (наприклад, перевірка даних бізнес-логіки та перевірка цілісності). Він також включає перевірку вручну для виявлення помилкових спрацьовувань і виклик зчитування для пояснення результатів.

Synopsys Software Risk Manager може керувати всіма цими інструментами аналізу AppSec, не сповільнюючи розробку. Використовуючи попередньо визначені політики ризиків, встановлені кожною організацією, він запускає правильні тести безпеки в потрібний час. Результатом є правильна інформація, яка надається розробникам і командам безпеки, щоб забезпечити відповідність їхнім політикам у всіх конвеєрах. Уніфікувавши політику, оркестровку тестів, кореляцію, пріоритезацію та вбудовані механізми SAST і SCA, організації можуть оптимізувати свою діяльність із забезпечення безпеки на підприємстві.

Команди безпеки також повинні розглянути модель розгортання для своїх інструментів тестування безпеки додатків. Традиційно компанії обирають локальне встановлення, щоб забезпечити контроль над своїми даними та інфраструктурою. З розвитком хмарних обчислень багато організацій використовують модель програмного забезпечення як послуги (SaaS), у якій їхні програми та дані розміщуються в хмарі. Основна перевага розгортання хмари полягає в зниженні витрат через наявність менше фізичного обладнання та інфраструктури для обслуговування, а також пов’язаних IT-команд для налаштування локальних інструментів. Крім того, використання інструменту безпеки додатків SaaS означає, що ваші накладні витрати на безпеку можуть еластично масштабуватися відповідно до вашого бізнесу.

Polaris Software Integrity Platform® — це інтегроване хмарне рішення для тестування безпеки додатків, оптимізоване для потреб розробки та команди vSecOps. Платформа Polaris об'єднує провідні на ринку механізми аналізу безпеки Synopsys в уніфіковану платформу, що дає вам можливість виконувати різні тести в різний час на основі програми, проекту, розкладу або подій SDLC.

За допомогою Polaris fAST Static ви можете знаходити та виправляти дефекти безпеки у власному коді та шаблонах інфраструктури як коду (IaC) за допомогою швидкого інкрементального сканування, яке забезпечує точні результати та значно скорочує час сканування.

Також з Polaris fAST SCA ви можете визначити вразливі місця в ланцюжку постачання програмного забезпечення вашого додатка за допомогою детальних рекомендацій Black Duck® Security Advisory (BDSA), які допоможуть вам оцінити серйозність і вплив, а також можливі варіанти вирішення проблеми та оновлення. Крім того, платформа Polaris дозволяє автоматизувати сканування та політику за допомогою інструментів DevOps, які ви використовуєте сьогодні. Це включає менеджери вихідного коду, такі як GitHub і GitLab, інструменти постійної інтеграції, такі як Jenkins, і інструменти відстеження проблем, такі як Jira.

– Реалізація:

Команда розробників збирає пакети, керує та розгортає випуски в різних середовищах.

– Розгортання:

Це етап, коли програмне забезпечення випускається у виробниче середовище.

– Керування:

Це етап, коли програмне забезпечення використовується у виробничому середовищі.

– Моніторинг:

На цьому етапі команда відстежує продуктивність програмного забезпечення, включаючи продуктивність системи, взаємодію з користувачем, нові вразливості системи безпеки та аналіз помилок або помилок у системі. Крім того, користувачам надсилаються оновлення або виправлення, щоб закрити вразливості або відповісти на нові загрози.

Ефективний SDLC не закінчується, коли продукт відправляється; воно продовжується протягом терміну корисного використання продукту. Хоча «вбудовування безпеки» під час розробки мінімізує помилки та інші дефекти, реальність така, що ідеального програмного забезпечення не існує. Таким чином, захист пристроїв IoT в першу чергу означає їх обслуговування.

4 ОЦІНКА ВРАЗЛИВОСТІ ПРИСТРОЇВ ІОТ

У цьому розділі надається практична оцінка вразливості конкретних пристроїв IoT за допомогою спеціальних інструментів.

У практичній частині цієї дипломної роботи ми проведемо оцінку безпеки конкретних девайсів Інтернету речей та розробимо та реалізуємо план підвищення їх безпеки. Нижче наведено загальний план практичної частини:

– Вибір пристроїв для оцінки безпеки: Визначення конкретних пристроїв IoT, які будуть об’єктом оцінки безпеки. Вибір може бути зроблений на основі популярності пристроїв, їх критичності для системи або потенційних ризиків.

– Аналіз вразливостей: Виконання тестування на проникнення, сканування вразливостей і аналіз потенційних ризиків безпеці для вибраних пристроїв.

– Реалізація заходів безпеки: Реалізація запропонованих заходів безпеки на вибраних пристроях. Це може включати встановлення оновлень програмного забезпечення, налаштування нових параметрів безпеки тощо.

– Перевірка ефективності заходів безпеки: Після впровадження заходів безпеки перевіряється їх ефективність. Це можна зробити за допомогою аналізу поточної безпеки пристрою, сканування вразливостей або інших методів оцінки.

– Документування результатів: опис результатів оцінки безпеки, впроваджених заходів безпеки та їх ефективності. Ця інформація буде використана для підготовки звіту про практичну частину дипломної роботи.

4.1 Оцінка вразливостей камери стеження за допомогою спеціалізованих інструментів

Для дослідження безпеки я буду використовувати камери спостереження Hikvision і Dahua російських користувачів, почнемо з огляду на загальні вразливості та експозиції (CVE) конкретних IP-камер, вироблених компаніями Hikvision і Dahua. Підключення IP камер до Інтернету взагалі є очевидним трендом. Враховуючи велику кількість IP-камер, розгорнутих у всьому світі, відносно невелика частка IP-камер, які знаходяться у відкритому доступі, може стати чудовим стимулом для хакерів.

Дослідити елементи мережі та перевірити безпеку сценарію збору інформації використовується сканер Nmap. Це безкоштовний інструмент із відкритим кодом для ідентифікації мережевих хостів і служб, для аналізу безпеки та аудиту мережі. Це найкращий інструмент для відображення реальних можливостей, що можуть бути використані мережі. Більша частина

гаджетів Інтернету речей не мають вбудованої системи безпеки, не мають вбудованого програмного забезпечення та оновлень безпеки. Ця відсутність безпеки є явною жилою для кіберзлочинців, які намагаються зламати безпеку мережі. Однак за допомогою функцій виявлення та аудиту Nmap можна швидко виявити та ідентифікувати хости чи пристрої в мережі та програмне забезпечення, що на них працює. Для пошуку потенційно вразливих пристроїв IoT використовуємо сканер Nmap. На рис. 4.1 наведено меню.

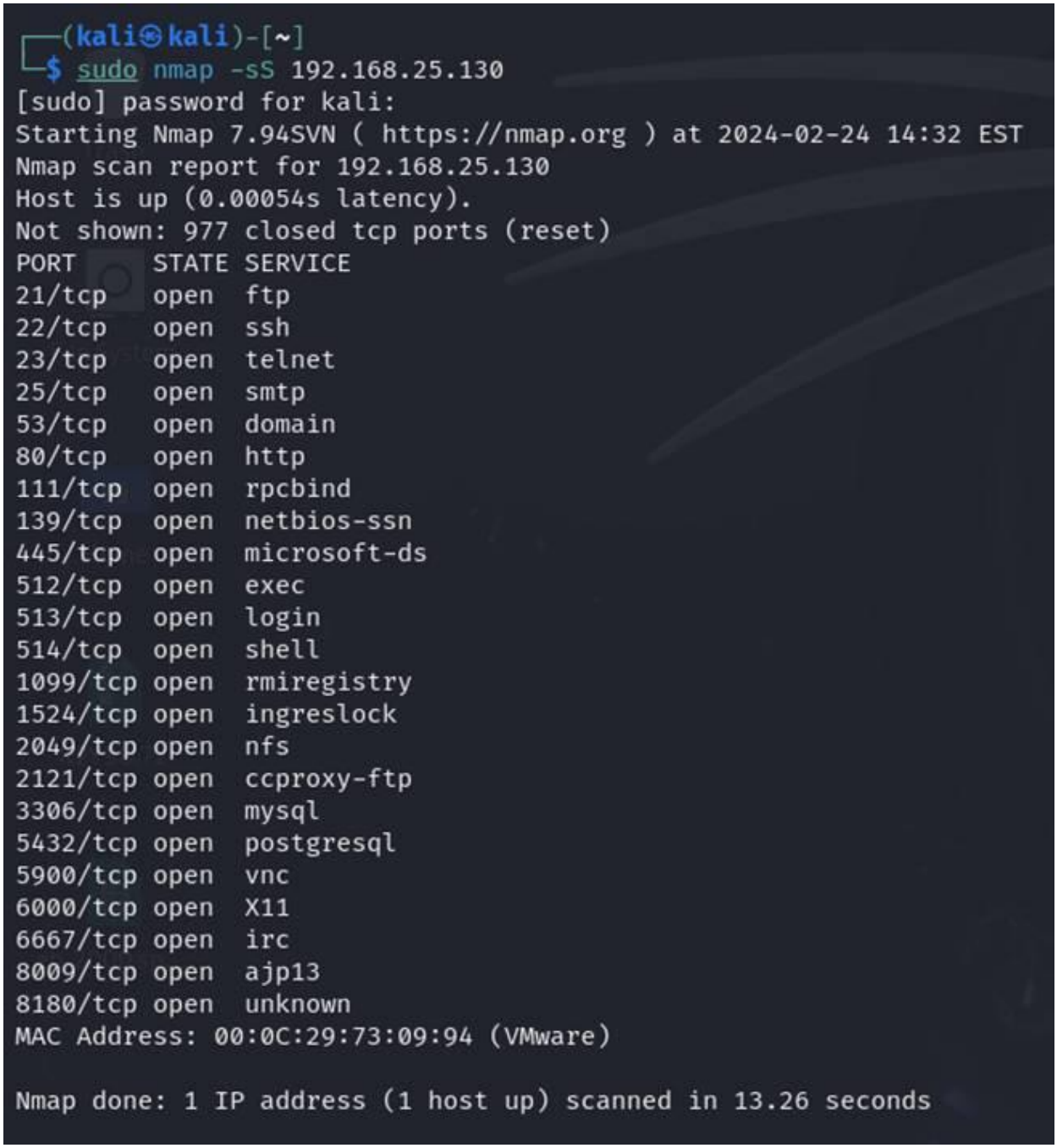


Рис. 4.1 Застосування пошуку Nmap

Router Scan — альтернативний інструмент для сканування елементів мережі. Дозволяє користувачам виявляти різні аспекти мережевих пристроїв,

такі як відкриті порти, служби, що працюють на цих портах, і потенційні вразливості або неправильні налаштування, які можуть становити загрозу безпеці. На рис. 4.2 відображено головне меню програми Router Scan

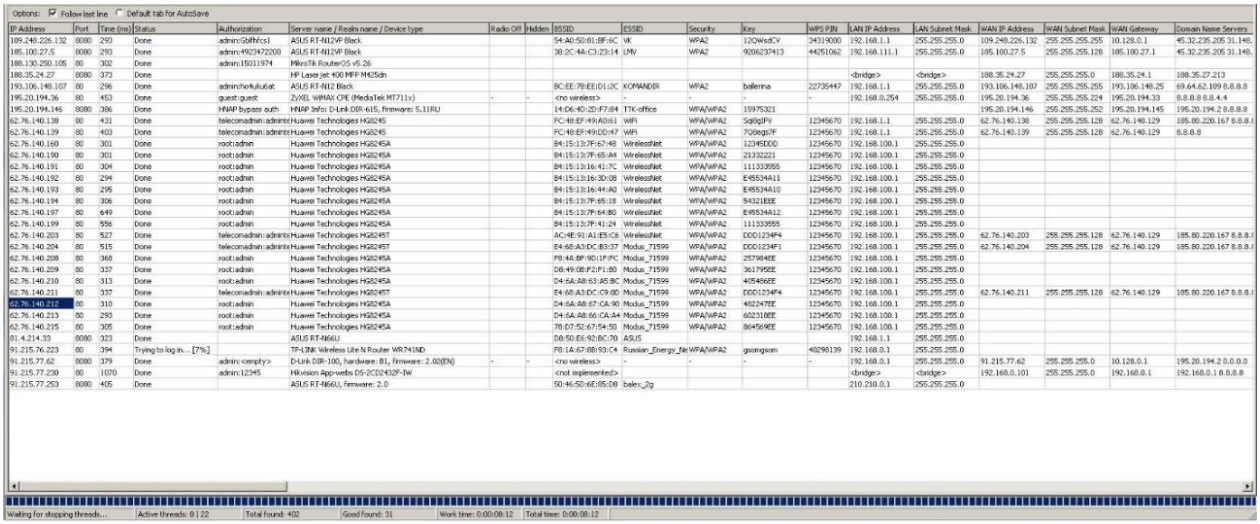


Рис. 4.2 вигляд програми Router Scan при скануванні

Також є можливість сканування пристроїв (IP-адрес у конкретному місті). Для цього використовуємо програму «4it.me» або іншу, що надає IP-діапазони усього світу. На рис. 4.3 зображено використання програми для адресів Києва.

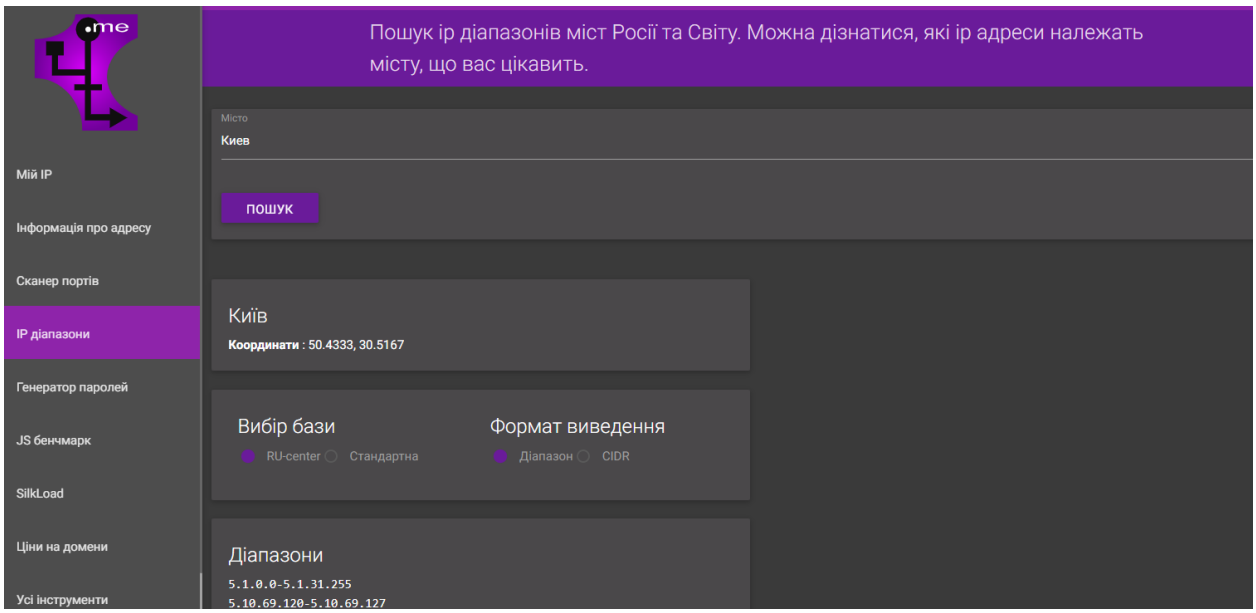


Рис. 4.3 Пошук айпі-адресів за допомогою сервісу

З рис. 4.3 є можливість переглянути найдені запити по містам, які надають місцезнаходження та діапазони IP-адрес, потім IP-адреси записуються у файл і запускається сканування утиліти Router Scan.

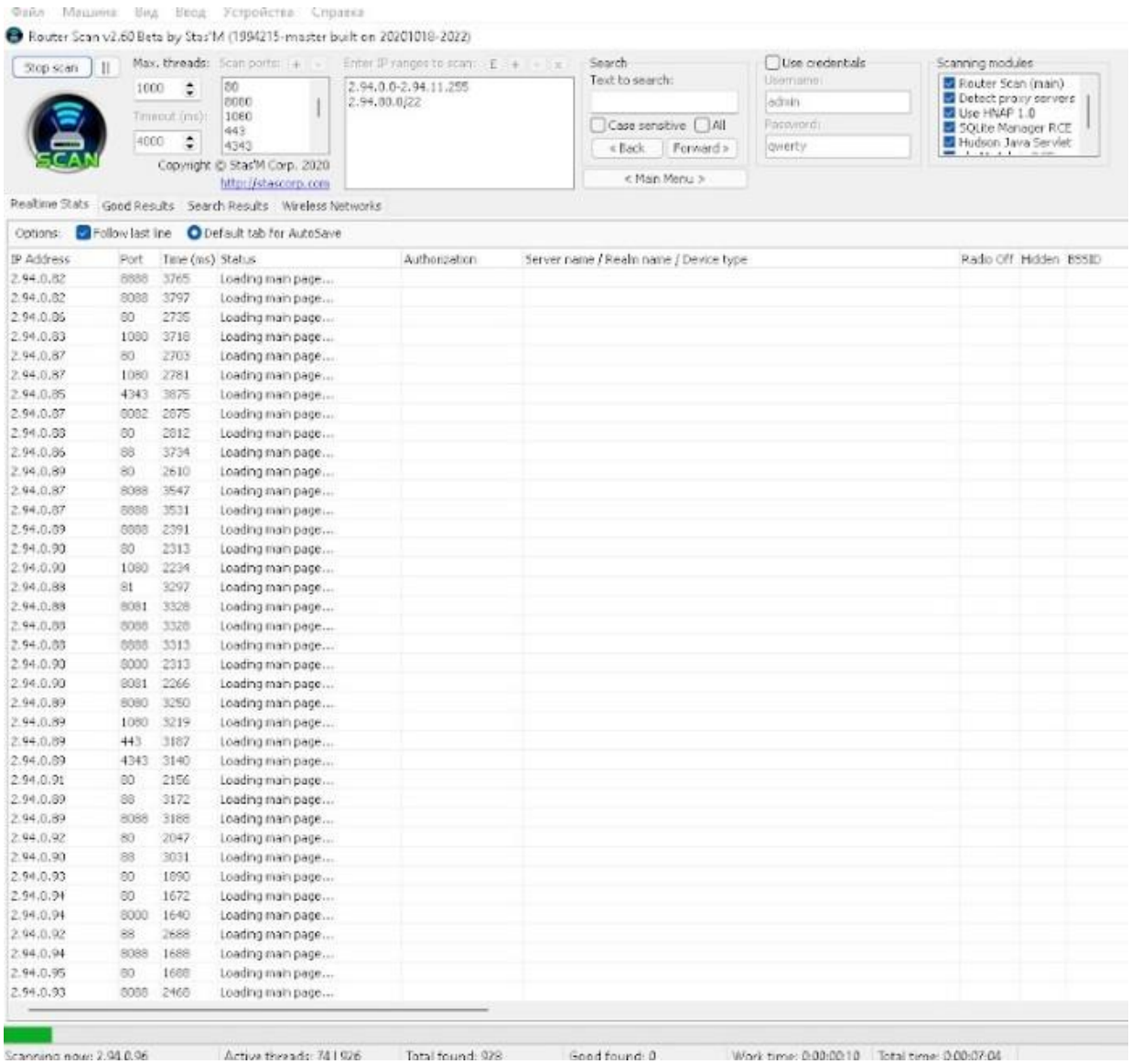


Рис. 4.4. Застосування програми Router Scan

З рис. 4.4 можна вгледіти відповідь на запит, доступні адреси, та порти.

Далі описані функції застосунку Router Scan:

Головна кнопка. Спочатку вона призначена для запуску тестування, проте потім функціонал було розділено на дві кнопки: одна для зупинки, а інша для паузи сканування.

Максимальна кількість потоків визначає, скільки пристроїв можна сканувати паралельно та одночасно. Цей параметр залежить від потужності робочої машини або віртуальної машини, на якій виконується сканування. Більша кількість потужності означає більше цінності.

Тайм-аут підключення. Встановлює поріг для очікування підключення до пристрою. Параметр доведеться інтуїтивно змінювати, щоб отримати стабільні результати сканування без втрати з’єднання. Якщо ви вважаєте, що програма використовує недостатньо потоків і система може надати більше ресурсів, спробуйте змінити режим сканування в налаштуваннях програми (за замовчуванням ми його не змінюємо).

Перелік портів для проведення тестування. Розкриває, які порти TCP перевірятимуться під час сканування діапазонів IP. Усі порти скануються за звичайним протоколом HTTP/1.0, за винятком портів 443, 4343 і 8443 — вони скануються через HTTPS за допомогою бібліотеки OpenSSL. Щоб збільшити кут огляду в мережі, можна додати до списку порти 81, 88, 8000, 8081, 8082, 8088, 8888 та інші. Також можна змінити список портів у файлі ports.txt.

Список діапазонів IP для сканування. Беремо їх з текстового файлу, в якому ми записали всі IP-адреси з сайту https://4it.me/getlistip, для якого міста ми зберегли адреси (в нашому випадку місто Курськ). Для зручності і щоб не перевантажувати машину, ми вибираємо кілька IP-адрес, а не всі відразу, і додаємо їх у форму 5 або в список діапазонів у файлі ranges.txt.

Далі, коли всі налаштування зроблені, запускаємо сканування, натиснувши кнопку 1. Дочекатися результату. У програмі внизу буде зелена смужка, яка вказує відсоток сканування. Також є дані про використаний і очікуваний час сканування. Використовуючи все це, за допомогою утиліти Router Scan було знайдено дані автентифікації пристрою Hikvision IoT та виявлено проблему вразливості безпеки Інтернету речей.

Головним інструментом пошуку будь-яких айпі, адресів, вразливостей та повного спектру інформації за пристроями є пошукова система Shodan. Це той самий гугл у світі Інтернет речей.

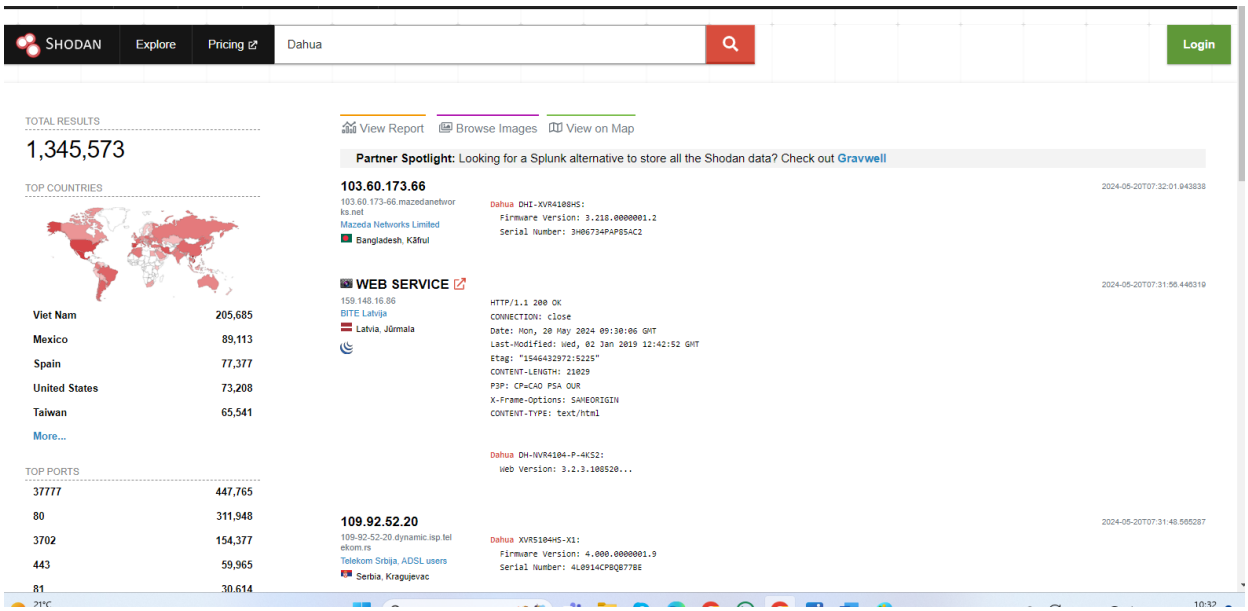


Рис. 4.5 Кількість пристроїв знайдених у мережі за запитом

З рис. 4.5 можна побачити кількість потенційно вразливих IoT-пристроїв постачальників продуктів і послуг відеоспостереження Dahua і Hikvision.

Виявлено IP-камеру Dahua версії 3.200.0001.6 (програмне забезпечення для мережевих камер) уразливість, класифікована як критична. Ця проблема

стосується невідомого коду. Невідоме маніпулювання введенням призводить до підвищення вразливості привілеїв. Помилка була опублікована 30.03.2017. Ця вразливість обробляється як CVE-2017-7253 від 24.03.2017. Атаку можна здійснити віддалено. Для роботи потрібна проста автентифікація. Розглянемо злом IP-камер Dahua версії 3.200.0001.6.

1) Використовування облікових даних з низьким рівнем прав за замовчуванням, щоб отримати список усіх користувачів

Ідентифікатор ресурсу (URI).

2) Вхід до IP-камери за допомогою облікових даних адміністратора, щоб отримати повний контроль над цільовою IP-камерою.

Ця вразливість має чотири етапи, а саме:

- виконує дамп бази даних віддалених користувачів;

- знаходить першого доступного користувача адміністратора та видаляє його логін і хеш пароля;

- запитує ідентифікатор сесії, обчислює новий хеш;

- виконує введення та виведення на/з віддаленого пристрою.

Сканер використовується для пошуку потенційно вразливих пристроїв IoT. На рис. 4.6 видно сканування мережі на наявність потенціального вразливого веб-серверу

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Dahua webcam httpd
|_http-favicon: Unknown favicon MD5: BD9E17C46BBBC18AF2A2BD718DDDAD0E
|_http-title: WEB SERVICE
| http-methods:
|_  Supported Methods: GET POST
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|WAP|router|VoIP phone
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X|2.4.X (96%), Excito embedded (91%), MikroTik RouterOS 6.X (89%), Drobo
embedded (89%), Grandstream embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/h:excito:b3 cpe:/o:linux:linux_kernel:4 cpe:/
o:linux:linux_kernel:2.4.20 cpe:/o:mikrotik:routeros:6.15 cpe:/h:drobo:5n cpe:/h:grandstream:gxv3275
Aggressive OS guesses: Linux 3.2 - 3.8 (96%), Linux 3.2 - 3.16 (93%), Linux 2.6.32 - 3.10 (93%), Linux 2.6.32 - 3.13 (91%
), Excito B3 file server (Linux 2.6.39) (91%), Linux 3.11 - 4.1 (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 2.6.33 (90%),
Tomato 1.27 - 1.28 (Linux 2.4.20) (89%), MikroTik RouterOS 6.15 (Linux 3.3.5) (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.219 days (since Sat Mar 19 06:09:03 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=241 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: webcam
```

Рис. 4.6 Сканування вразливого девайсу за допомогою сканеру

З рис. 4.6 можна побачити відкритий порт 80, тобто службу HTTP, на якій встановлено веб-сервер на операційній системі Linux для відеоспостереження Dahua. Використовуючи підтвердження концепції, тобто вразливість CVE-2017-7253, було проведено дослідження веб-сервера, зображено на рис. 4.7.

Рис. 4.7. Застосування експлойту до камери

Як видно з рис. 4.7 дослідження здійснюється на веб-сервері, де програмне забезпечення робить запит на сервер для встановлення версії, у такій ситуації сервер використовує другу версію/генерацію, після чого виконується віддалений дамп бази даних неліцензіованих користувачів і відображає першого доступного користувача адміна з його ніком і хешем пароля. Після отримання паролю та назви ввійшли на данний девайс, програмне забезпечення запитує ідентифікатор сеансу. Це все зображено на рис. 4.8

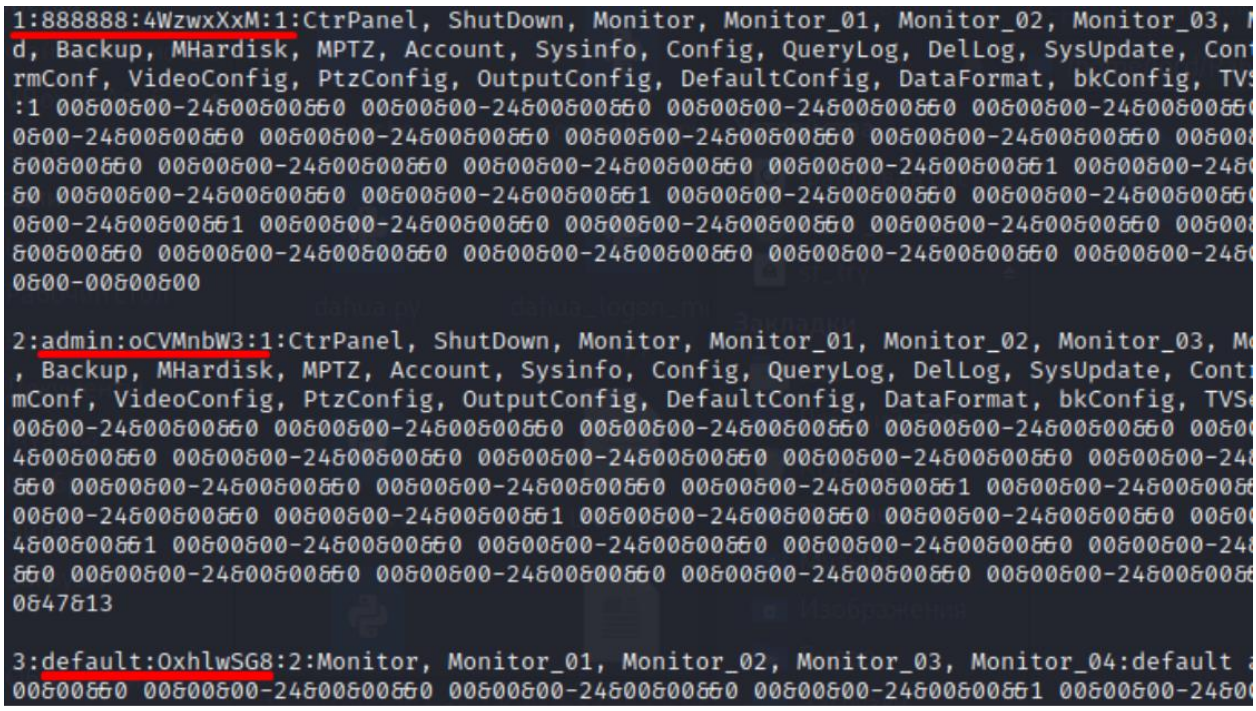


Рис. 4.8 Данні надані за кожним користувачем

З рис. 4.8 можемо побачити всю базу даних віддалених користувачів із усіма доступними обліковими записами, по якій пристрої зламують, є наявність слабкого пароля або пароля за замовчуванням. Рекомендується змінити стандартний пароль на складний. Перший і третій облікові записи є

жорстко закодованими паролями, іншими словами, логін і пароль вбудовані і не можуть бути видалені. Для другої версії програмного забезпечення продукту 48-розрядний алгоритм Dahua використовується для зміни відкритого пароля в хеш, а третя версія використовує алгоритм 5-го покоління Message-Digest (MD). Виходячи з цього, хеш підходить до публічного паролю. Вибрати пароль можна за допомогою програмного забезпечення John The Ripper (JtR).

JtR — популярний інструмент злому паролів, який можна використовувати для здійснення атак методом грубої сили з використанням різних технологій шифрування та корисних списків слів.

Приклад використання JtR для вибору хеш-паролю за 48-бітним алгоритмом Dahua наведено на рис. 4.9.

Програмне забезпечення містить кілька модулів для генерації хешів із різних типів файлів, таких як ключі Secure Shell (SSH) із ssh2john, файли .kbdx із keepass2john та захищені паролем zip-архіви з zip2john. Потім ви можете використовувати ці хеші як вхідні дані, щоб знайти пароль. Є реалізації для різних операційних систем. Дуже популярний завдяки підтримці великої кількості хешів, авторозпізнаванню хешу та налаштованому зломщику. Також підтримує багато модулів, у тому числі сторонніх.

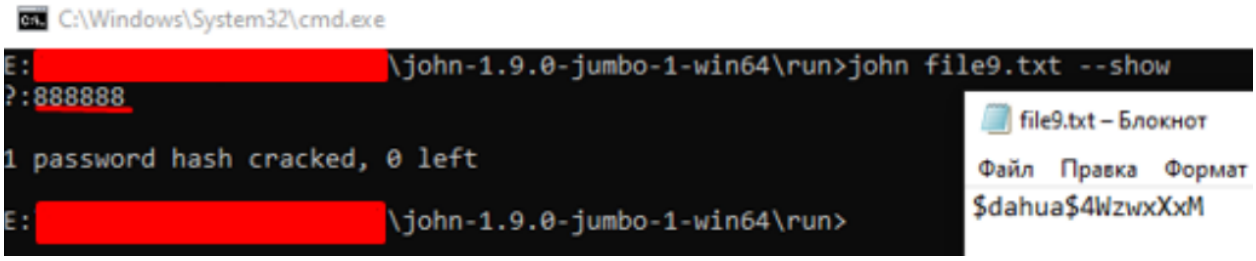


Рис. 4.9 Використання JtR для підбору пароля

Можна зробити висновок, що в даному випадку не дотримуються основних правил безпеки. CVE-2017-7253 — це застаріла вразливість, тому вона рідкісна, але становить критичний рівень загрози.

Використання застарілого програмного забезпечення та несвоєчасне його оновлення призводить до системних проблем. Контроль доступу було порушено, оскільки стандартні паролі та стандартні порти не змінювались під час налаштування.

Сканування гаджетів IoT на наявність уразливостей CVE-2021-3304. У деяких продуктах Dahua під час входу в систему виявлено вразливість обходу автентифікації.

Зловмисники можуть обійти автентифікацію пристрою шляхом створення шкідливих пакетів даних.

```
# Authentication bypass start
if logon == "netkeyboard":
    """ 'CVE-2021-33044, Authentication bypass,
    when setting param: 'clientType": "NetKeyboard' """
    params.update({
        "clientType": "NetKeyboard"
    })
    return params

elif logon == "loopback":
    """ loginType=5, @127.0.0.1 """
    """
    'CVE-2021-33045, Authentication bypass,
    when setting params: 'ipAddr':'127.0.0.1', 'loginType': 'Loopback' and 'clientType': 'Loca
    Note: Bypass fixed with newer firmware from beginning/mid 2020

    Legit usage: SNMP daemon traffic on 127.0.0.1 using port 5000 with l/p admin/admin
    """

    dh_hash = dahua_gen2_md5_hash(
        username=username, password=password, dh_realm=dh_realm, dh_random=dh_random,
        saved_host=saved_host)

    params.update({
        "loginType": "Loopback",
        "clientType": "Local",
        "passwordType": "Default",      # Plain working too
        "password": dh_hash     # Clear text password working too with 'passwordType': 'Plain'
    })

    return params
# Authentication bypass end
```

Рис. 4.10 Надсилаючі спеціально створені пакети даних на цільовий пристрій

Уразливість CVE-2021-33044 працює на тих пристроях, які її не підтримують функціональні можливості «NetKeyboard» старіші за перший місяць двадцять першого року, у той час версія мікропрограми CVE-2021-33045 старіша за початок/середину 2020 року.

Крім того, програмне забезпечення дозволяє будь-якому користувачеві низького рівня отримати повний доступ до консолі за допомогою анонімного входу.

За для аналізу безпеки пристроїв Dahua IoT була обрана пошукова система система Shodan, яка наведена на рис. 4.11.

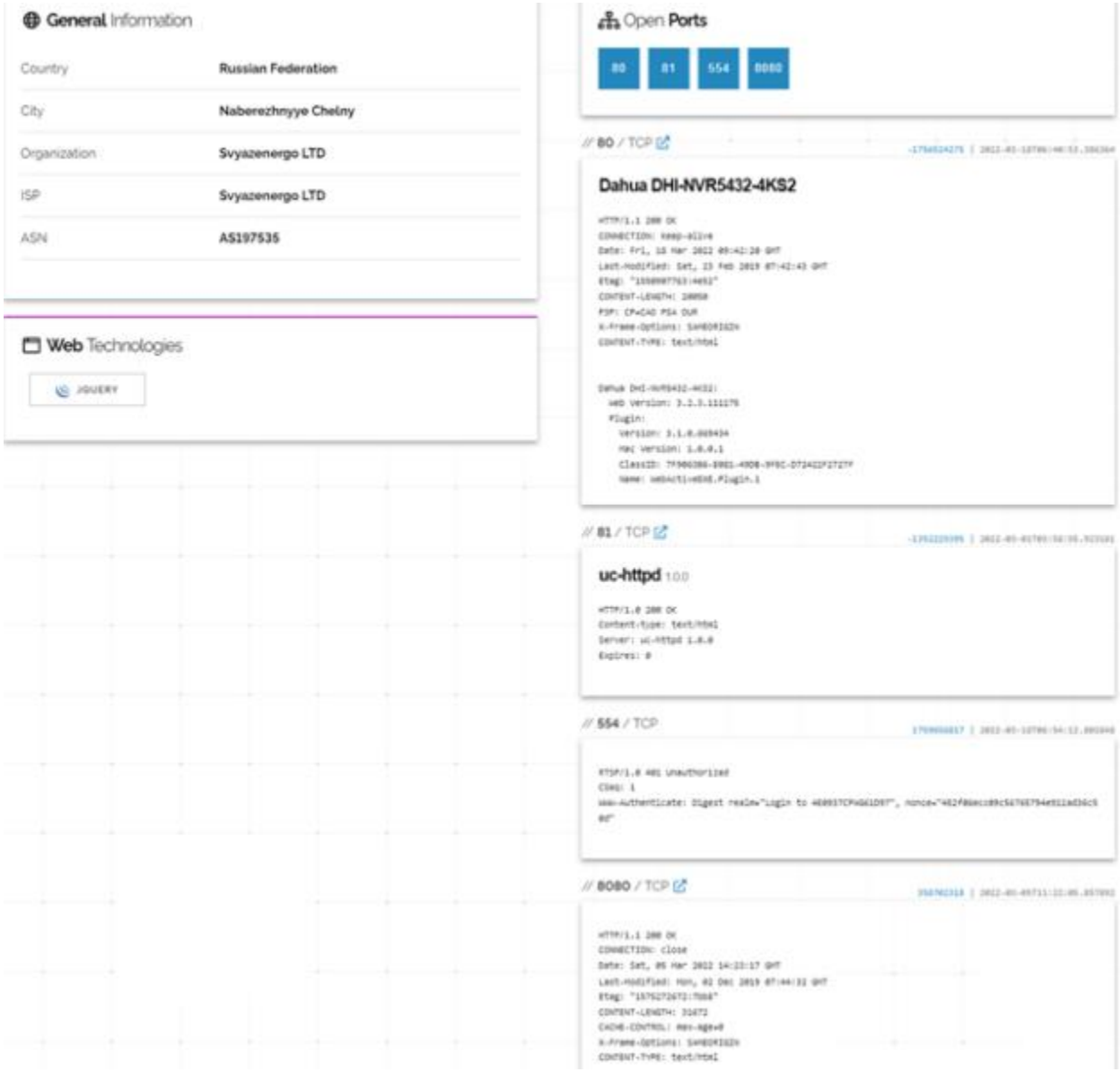


Рис. 4.11 Використання Шодану для отримання повної інформації

З рис. 4.11 можна побачити, що власник користується кількома відкритими портами з різноманітними службами, де основний веб-сервер використовується на порту 80. Використовуючи отримані дані, CVE-2021-33044 було використано через HTTP на порту 8080, результати можна спостерігати на рис. 4.12.

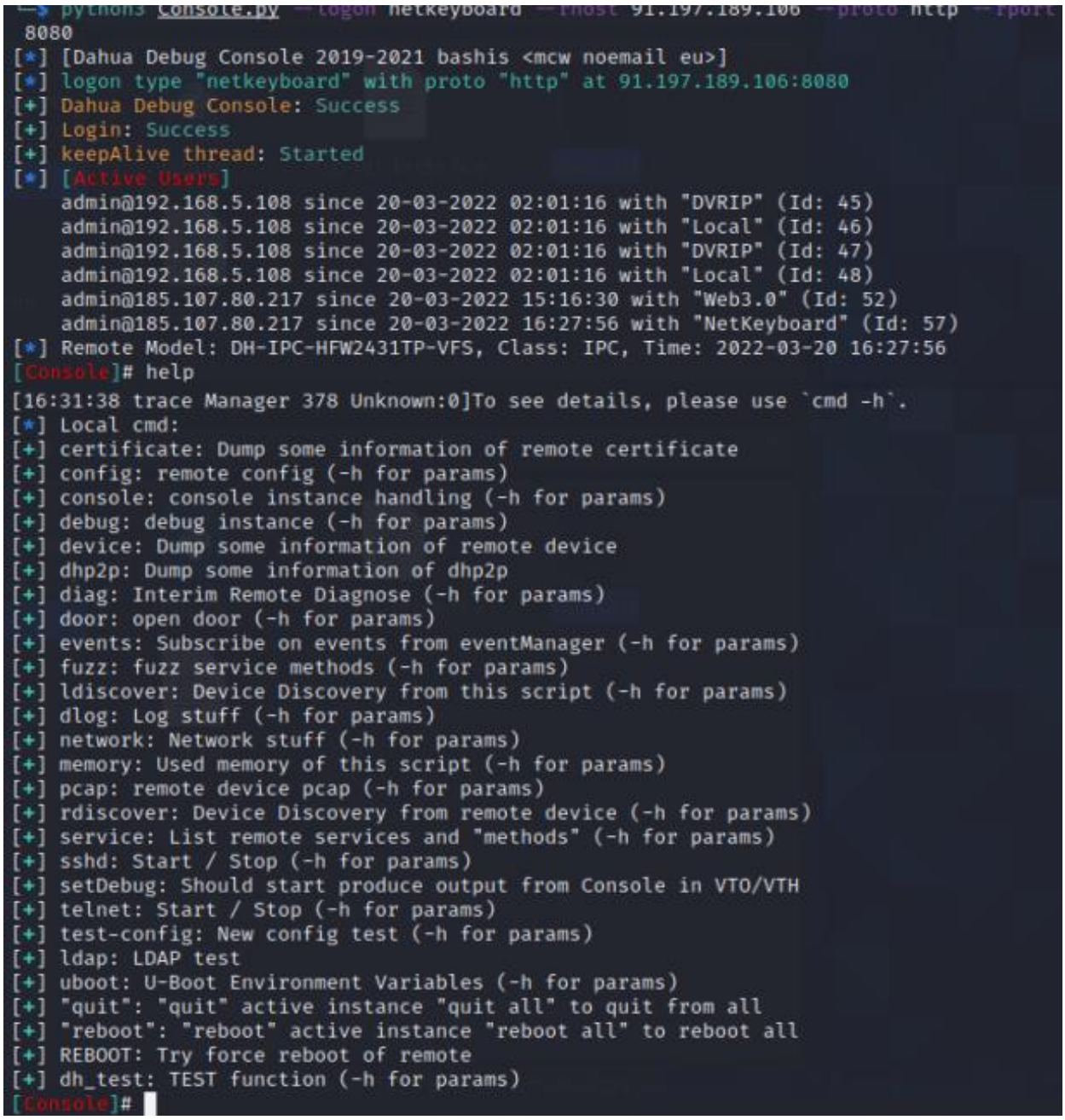


Рис. 4.12 Результати використання експлойту

На рис. 4.12 бачимо успішну авторизацію. В тому числі, програмне забезпечення забезпечує широку функціональність, а саме створення дампа файлів конфігурації системи сертифікату, підключення Telnet, SSH та інші можливості.

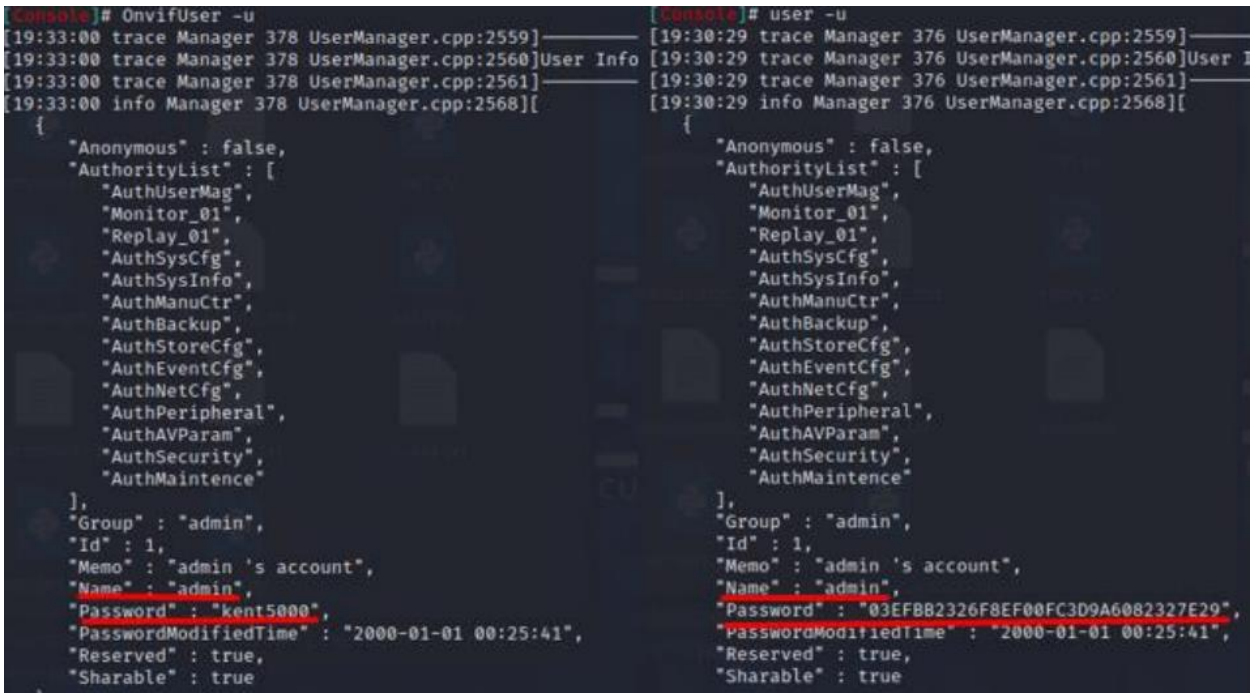


Рис. 4.13 Бачимо скинутий хеш пароля та відкрити пароль

На рис. 4.13 видно, що програмне забезпечення камери Dahua залишає пароль не лише в хешованій формі, як і у відкритій формі, це становить загрозу захисту конфіденційність даних. Додаткові докази недостатнього захисту конфіденційність даних – це збереження паролів бездротових мереж, Peer-to-Peer, File Transfer Protocol, Telnet та різних сервісів, спричиняє виникнення нових можливостей кіберзлочинів.

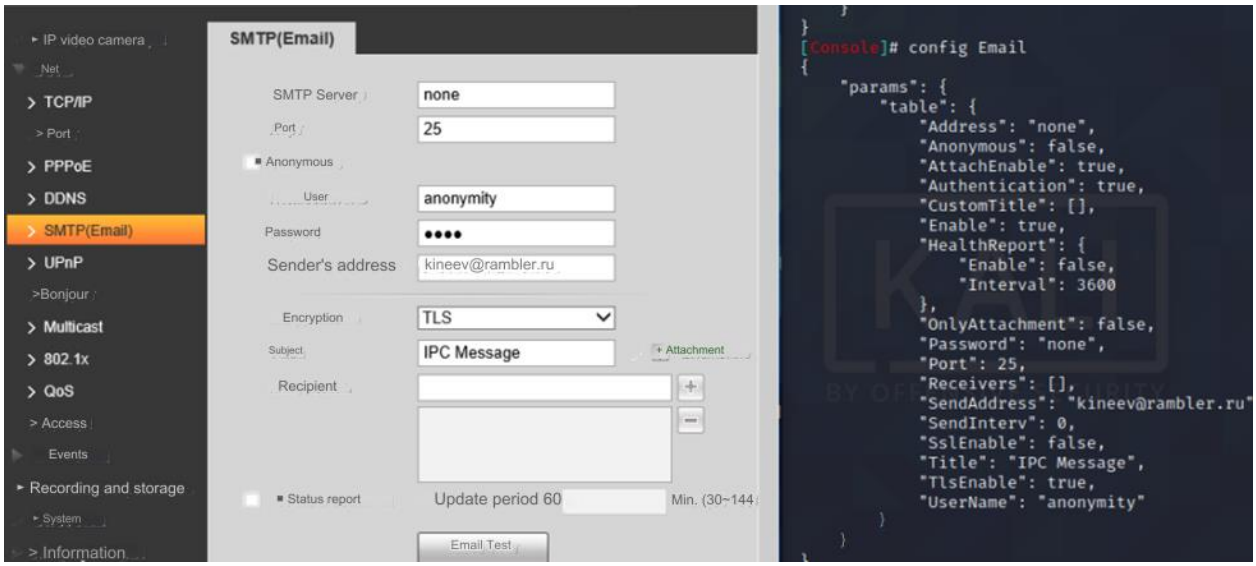


Рис. 4.14 Збереження адреси електронної пошти

Зберігання записів відеоспостереження на карті Secure Digital (SD) додає додатковий шар захисту для конфіденційних даних. Це через те, що фізичний периметр безпеки, який створюється зберіганням на SD-карті, легше захистити від потенційних фізичних загроз, ніж захист на рівні мережі.

У порівнянні з хмарними сервісами зберігання даних, які можуть стати каналом витоку інформації, або використанням FTP-сервера, яке може бути не досить безпечним з точки зору інформаційної безпеки, зберігання на SD-карті може бути більш захищеним варіантом.

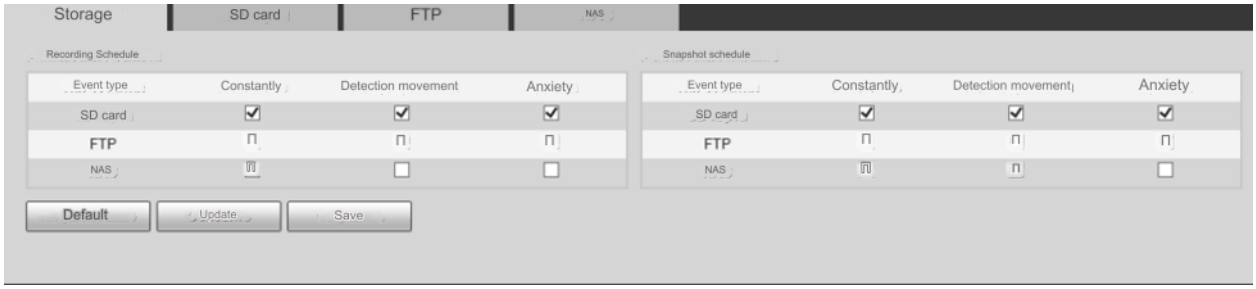


Рис. 4.15 Налаштування зберігання записів відеоспостереження

Виконано використання отриманих даних аутентифікації з порту 8080, увійшов на головний веб-сервер через порт 80, дані автентифікації аналогічні в різних пристроях. Використання однакових паролів для кожного пристрою створює критичне значення загрози з точки зору контролю доступу.

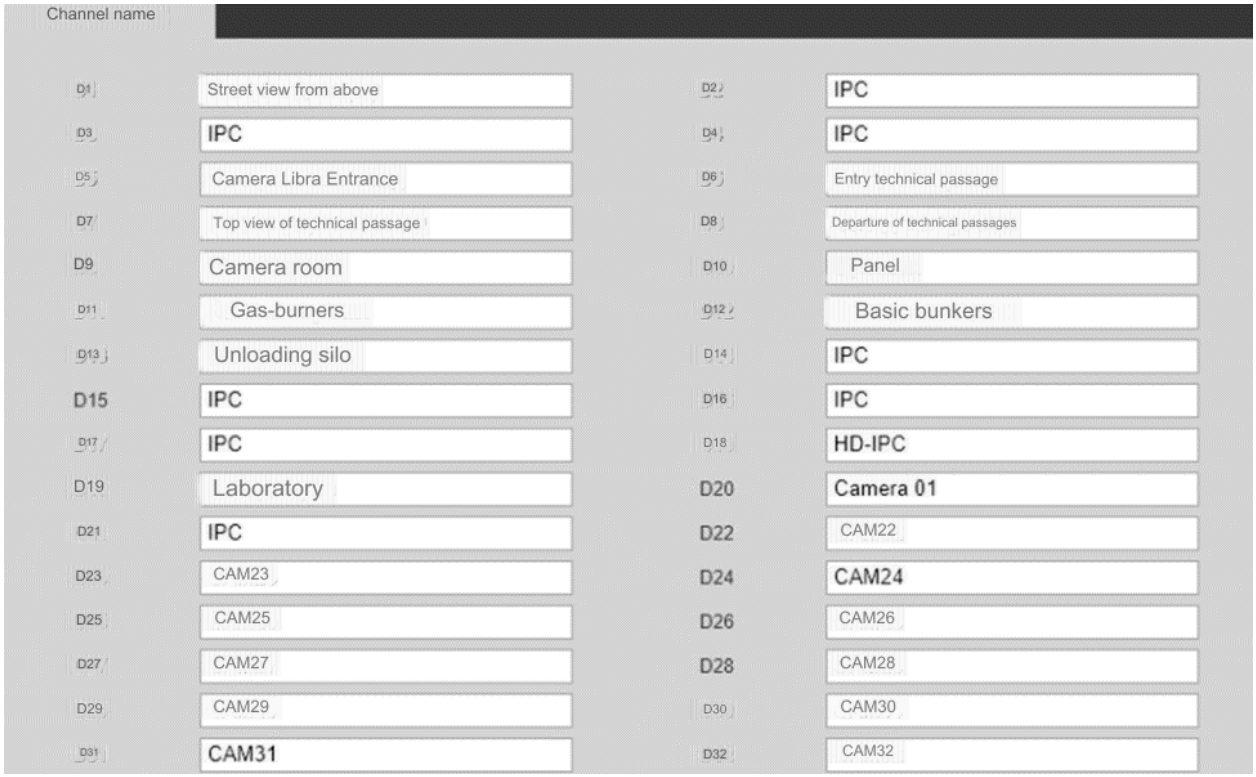


Рис. 4.16 Назви каналів передачі даних відеоспостереження головного веб-сервера

Ще один метод стеження за атаками - аналіз журналу подій безпеки.

Являє собою важливе місце для зберігання журналів безпеки системи, яке використовується для керування безпекою системи та її аудиту. Один із методів діагностики критичних станів системи полягає у постійному аналізі

системних журналів у режимі реального часу. Це через те, що інформація, що міститься в цих журналах, відображає стан системи, її ресурси, а також дії користувача. Проте, під час налаштування було виявлено, що веб-сервер не використовує системний журнал, що припиняє керування та аудит безпеки системи та створення відповідних заходів протидії потенційним кібератакам.

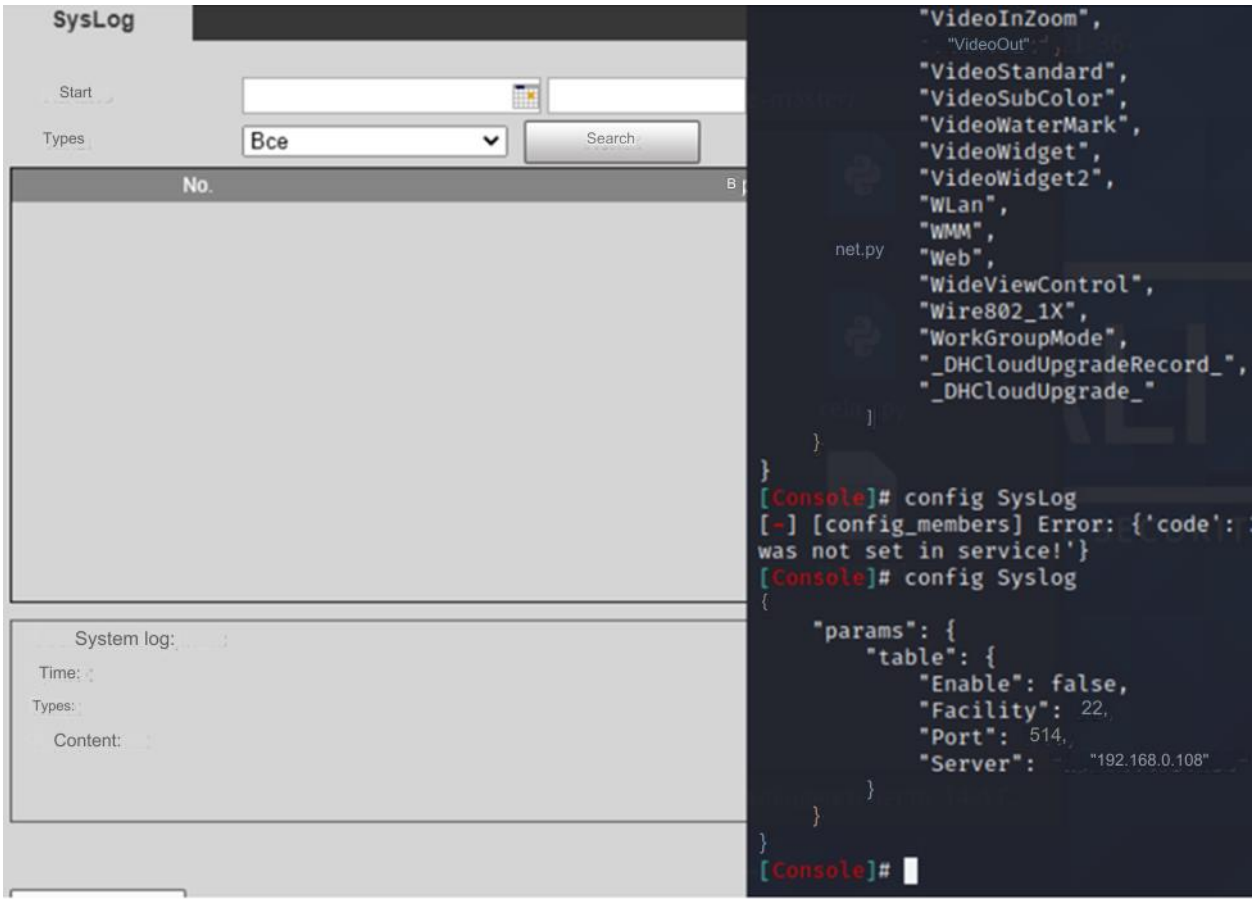


Рис. 4.17 Перегляд параметрів системного журналу

Що стосується безпеки, налаштування веб-безпеки було досліджено на сервері, який зображено на рис. 4.18.

На рис. 4.18 показано такі параметри безпеки: IP-фільтрація, обслуговування системи та налаштування протоколу HTTPS.

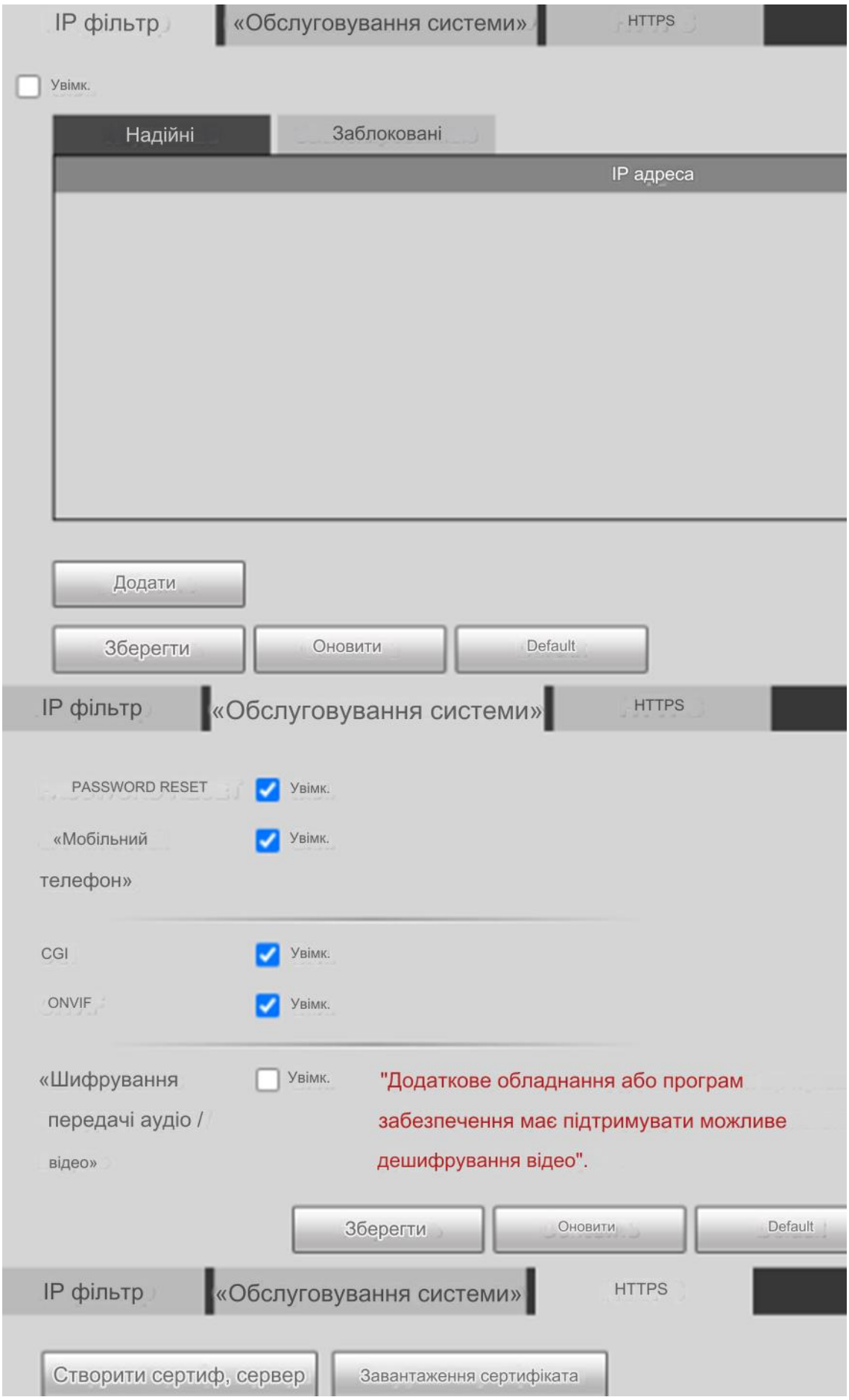


Рис. 4.18 Налаштування веб-безпеки

IP-фільтрація дозволяє обмежити доступ, який, у свою чергу, не призведе до компрометації системи, знаючи дані аутентифікації.

Що стосується обслуговування системи, то є можливість відновлення пароля, можливість керування пристроєм через мобільний телефон, а також підтримка протоколів CGI і ONVIF для спрощення інтеграції зі стороннім програмним забезпеченням, для полегшення вибору кінцевого користувача, купуючи девайси конкретного виробника, треба бути впевненим в їх сумісності з іншим програмним забезпеченням, це в кінцевому підсумку дозволяє розширити доступність та відкритість ринку систем відеоспостереження для різних споживачів.

Також є можливість створення та завантаження на сервер самопідписаного або автентифікованого сертифікату X.509, а саме змінити на протокол HTTPS, протокол забезпечує безпечний зв'язок між користувачем і сервером навіть у незахищеній мережі за допомогою SSL і криптографічних протоколів TLS.

Тому ця версія програмного забезпечення пристрою Dahua не має широкого спектру методів забезпечення інформаційної безпеки. Більше того, навіть доступні заходи безпеки не були застосовані. Базові вимоги щодо контролю доступу, захисту поверхні атаки, використання актуального програмного забезпечення, шифрування і захисту конфіденційних даних не були дотримані. Це створює серйозні ризики безпеки, оскільки такий пристрій стає привабливою мішенню для зловмисників.

Аналізуючи розглянуті методи з урахуванням відомих вразливостей CVE-2021-33044 та CVE-2021-33045, робимо висновок, що виявлені вразливості мають критичний рівень, який негативно впливає на конфіденційність, цілісність і доступність системи. Конкретно, їхня експлуатація може призвести до повного розкриття інформації, порушення цілісності системи та повної втрати захисту, а також повного відключення ураженого ресурсу, що може зробити його повністю недоступним.

Після проведення сканування пристроїв IoT на предмет вразливостей CVE-2021-36260 було виявлено, що деякі продукти Hikvision містять уразливості, пов'язані з недостатньою перевіркою вхідних даних веб-сервером. Це дозволяє зловмисникам впроваджувати шкідливі команди через віддалені атаки.

Виявлені уразливості впливають на більшість останніх моделей IP-камер Hikvision, які можуть бути вразливими до атак без автентифікації. Ці атаки дозволяють зловмисникам виконувати команди в системі з підвищеними привілеями.

```
def put(self, url, query_args, timeout):
    query_args = '<?xml version="1.0" encoding="UTF-8"?>' \
                 f'<language>$({query_args})</language>'
    return self.remote.put(self.uri + url, data=query_args, verify=False, allow_redirects=False, timeout=timeout)
```

Рис. 4.19 Редакція коду PoC, що показує введення команди на веб-сервер

Ця уразливість дозволяє кіберзлочинцю отримати повний контроль над пристроєм і наділити його необмеженими правами кореневого доступу. Це надає значно більший рівень доступу, ніж у власника пристрою, який обмежений "захищеною оболонкою" - Perl Shell (psh), що фільтрує вхідні дані за попередньо визначеним набором обмежених, переважно інформаційних команд.

Крім того, вразливість може призвести до повної компрометації IP-камери і отримання доступу до внутрішніх мереж, що відкриває можливості для подальших атак. Являє собою критичну вразливість найвищого рівня – уразливість неавтентифікованого віддаленого виконання коду, вона впливає на велику кількість камер Hikvision, при цьому власник пристрою не потребує ніяких дій. Це створює загрозу для підключених внутрішніх мереж, що в свою чергу розкриває нові вектори кібератак. Розгортання таких камер на важливих об’єктах може навіть загрожувати критичній інфраструктурі.

Ця уразливість має критичний рівень і впливає на конфіденційність, цілісність і доступність системи. Конфіденційність порушується через повне розкриття інформації, що призводить до викриття всіх системних файлів.

Цілісність порушується через повне порушення цілісності системи, що призводить до повної втрати захисту системи і компрометації всієї системи. Доступність також порушується через повне відключення зламаного ресурсу, що дозволяє зловмиснику зробити ресурс повністю недоступним.

Для перевірки цієї вразливості необхідно мати доступ лише до порту сервера HTTP/HTTPS, який зазвичай використовується (80 або 443). Ім'я користувача та пароль не потрібні, і власник камери не має виконувати жодних дій. Навіть реєстрація на самій камері не допоможе виявити цю вразливість. З цією метою було здійснено пошук тридцяти п'яти потенційно вразливих пристроїв IoT за допомогою пошукової системи Shodan, один із прикладів яких наведено на рис. 4.20.

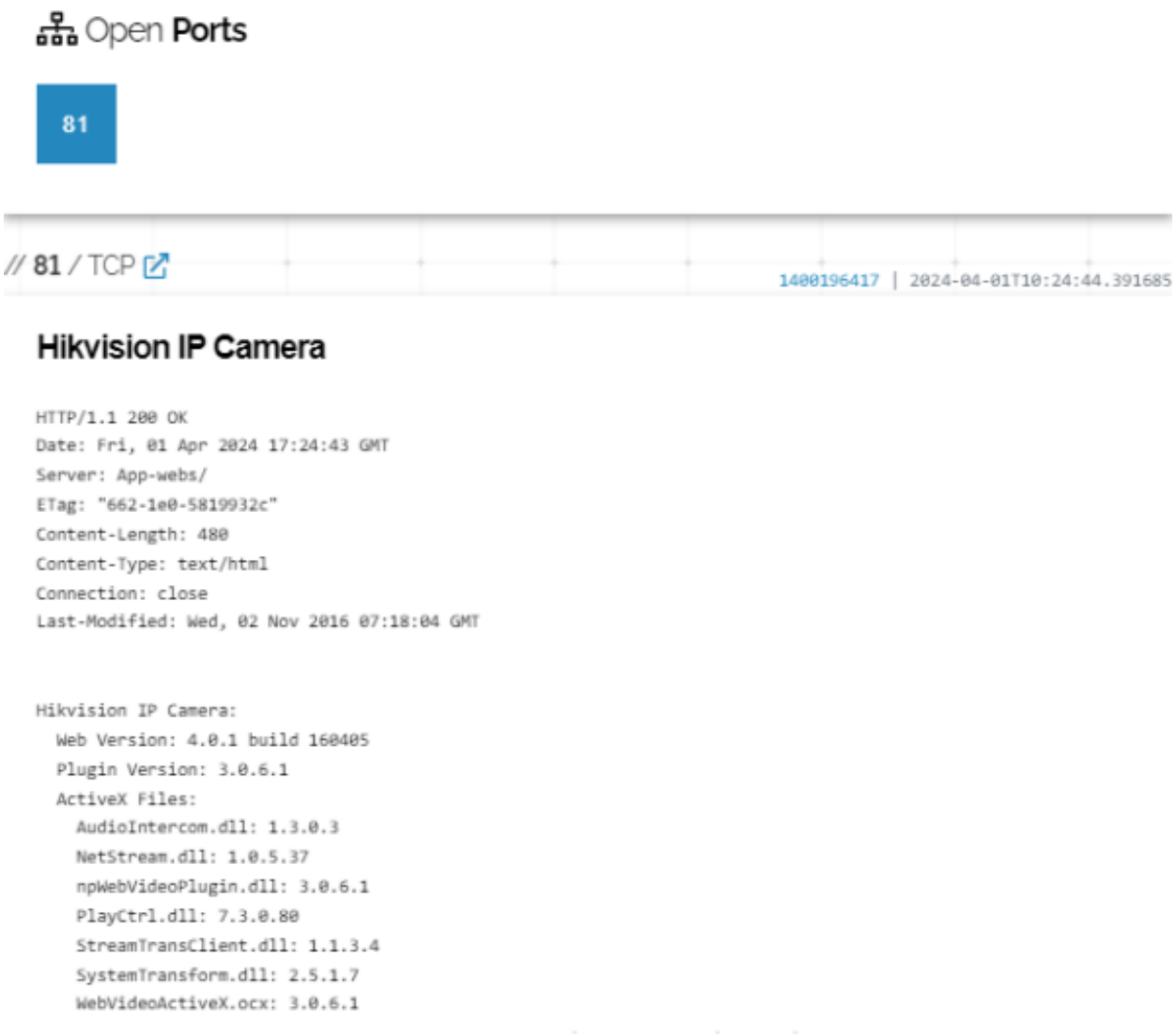


Рис. 4.20 Інформація за 81 портом

За рисунком 4.20 бачимо, що хост має відкритий порт HTTP-сервера, який останній раз оновлювався у 2016 році, що може свідчити про потенційну вразливість пристрою.

Щодо інших пристроїв IoT, які були просканованні, виявлено, що вони мають кілька відкритих портів, при цьому щонайменше один сервер мав застаріле програмне забезпечення. Це вказує на широку область застосування атаки. Після отримання необхідної інформації було проведено дослідження вразливостей, які відображаються на рис. 4.21.

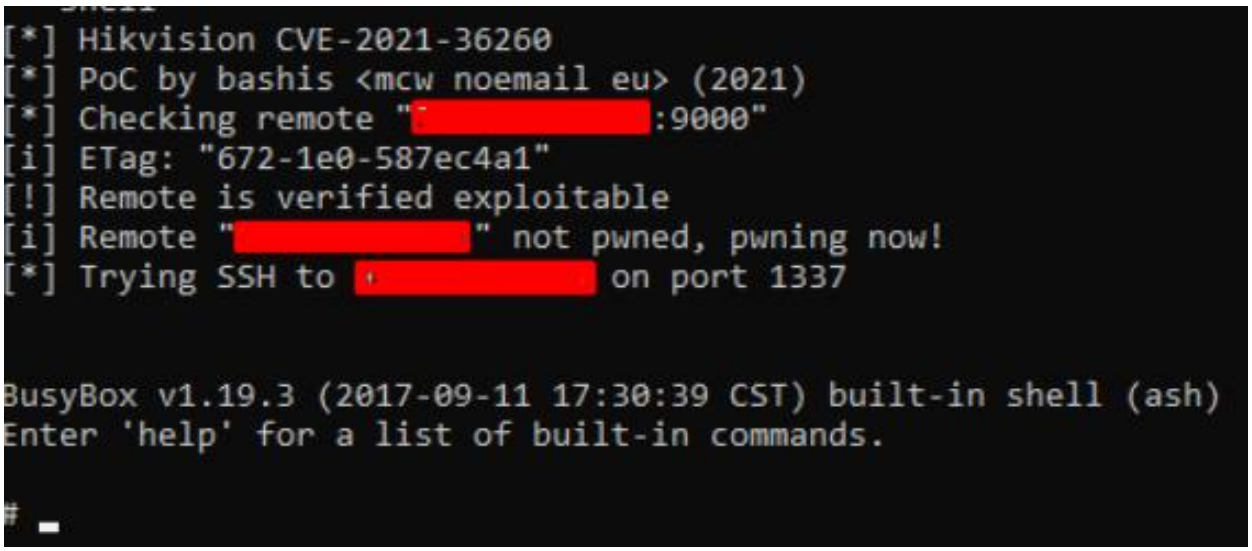


Рис. 4.21 Успішне використання експлойту

На рисунку 4.21 видно застосування вразливості. Перше програмне забезпечення спочатку перевіряє доступність пристрою, а потім наявність вразливості у два етапи: спочатку воно перевіряє, чи є камера Hikvision кінцевою точкою, а потім перевіряє, чи правильно камера реагує на експлуатацію. У цьому випадку камера виявилася вразливою, тому виконується ін'єкція.

Команда HTTP PUT надсилається в корисне навантаження XML, де можна використовувати з'єднання оболонки SSH або виконати команду всліпу як команду. В результаті отримуємо обмежену оболонку з двадцятьма чотирма вбудованими командами та десятьма різними параметрами командного рядка.

Ця оболонка може бути використана для тестування сценаріїв на сумісність оболонки, а також для перегляду детальної інформації про вміст каталогів, що зберігаються на пристрої.

На рисунку 4.22 показано вигляд поточного каталогу. Можливість переглядати та змінювати системні файли без проходження процесу автентифікації підтверджує концепцію критичної вразливості.

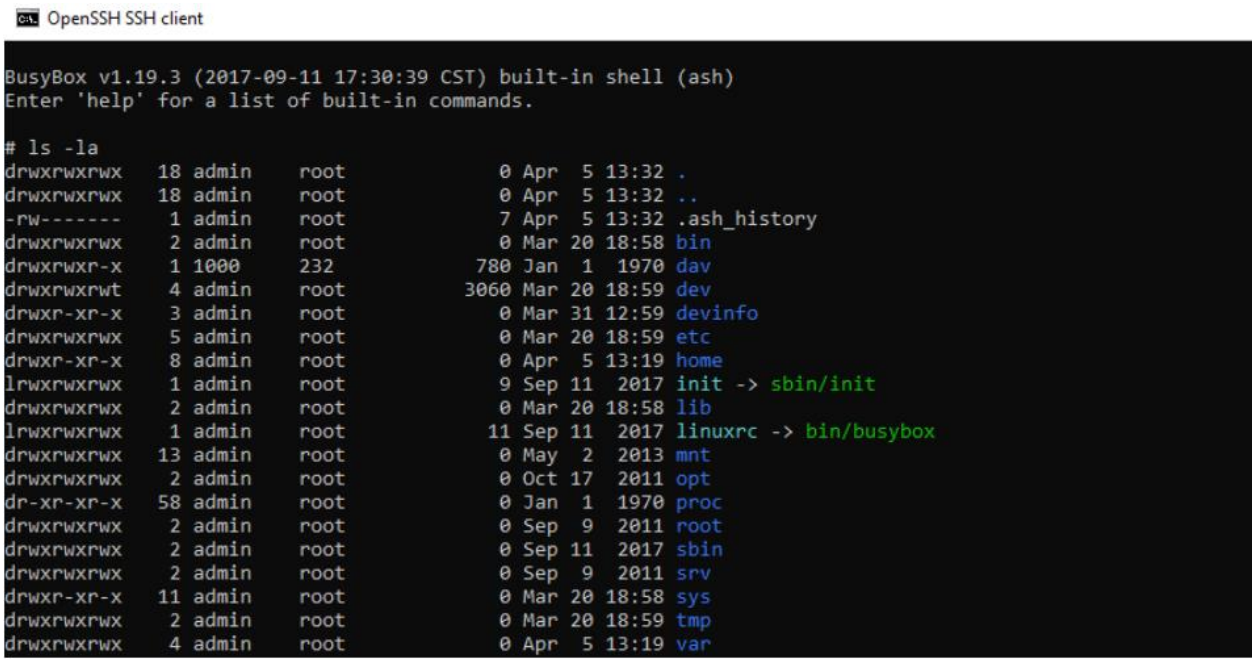


Рис. 4.22 Файли системи

На рис. 4.22 зображено перелік файлів системи, в яких відображається доступ і редагування таких файлів, отже, це потенційна загроза. основними властивостями інформації якої є об’єкт захисту, а саме: цілісності, конфіденційності та доступності. Цікавими файлами, які складають дані конференції, є каталоги, у яких зберігаються інформація про пристрій і дані. Перегляд файлів, розташованих у репозиторії dev info, наведено на рис. 4.23.

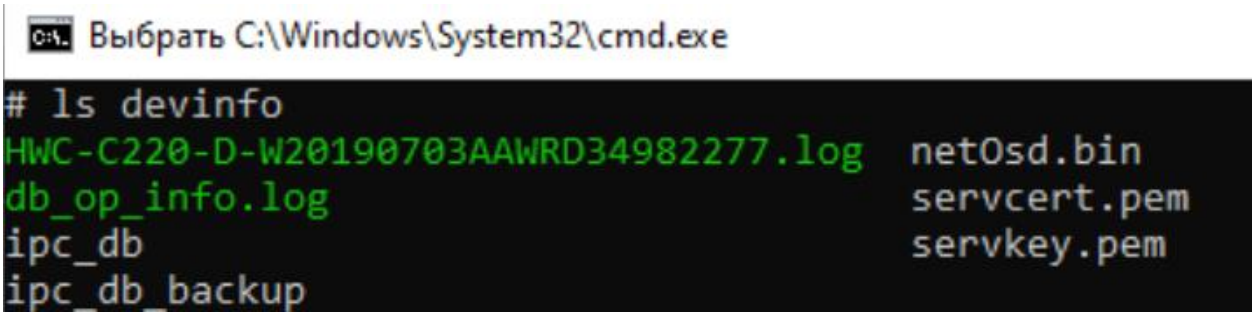


Рис. 4.23 Данні з репозиторію devinfo

У репозиторії dev info також були виявлені список файлів, що мають такі назви: ipc_db, та ipc_db_backup, які являють собою бази даних формату SQLite. Ці файли зберігаються у місці знаходження відкритих паролів, даних внутрішньої мережі, службових даних та іншої інформації. Показано на рис. 4.24.

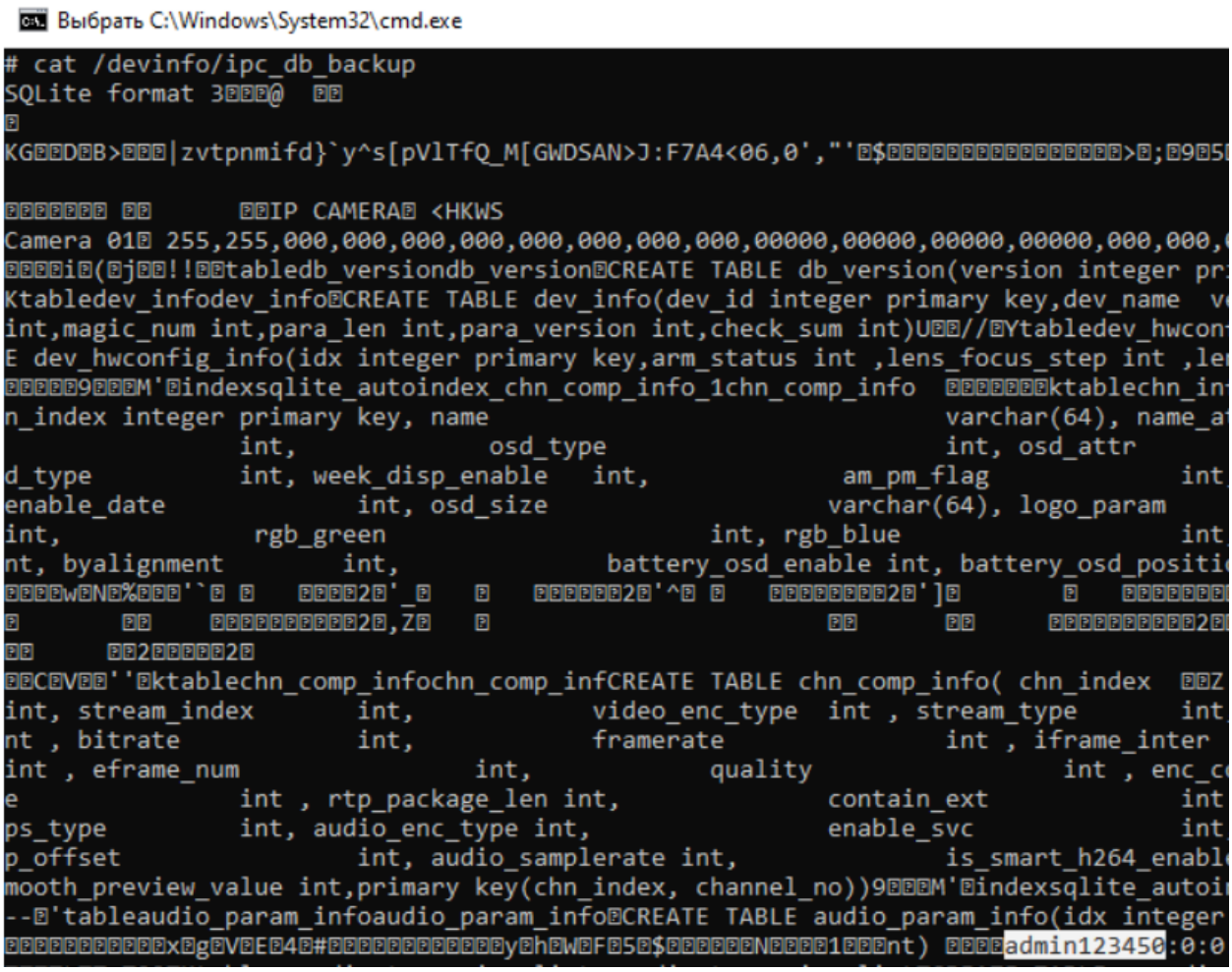


Рис. 4.24 Данні камери

З рис. 4.24 бачимо характеристики, налаштування камери та наявний пароль.

Що стосується вищезгаданого каталогу, то описаний каталог "/etc" є частиною файлової системи та містить конфігураційні файли більшості системних утиліт і програм. Однак, файл "/etc/passwd" є особливо цікавим для зловмисників, оскільки він містить список облікових записів користувачів у текстовому форматі. Його основна мета полягає в тому, щоб зіставити імена користувачів з їх ідентифікаторами, при цьому поле пароля містить хеш-код пароля, який використовується для автентифікації.

Кожен рядок у файлі описує окремого користувача та містить сім полів, розділених двокрапками: ім'я для входу або логін, хеш пароля, ідентифікатор користувача, групи за замовчуванням, інформаційне поле, домашній каталог та оболонку входу. Ви можете побачити приклад перегляду файлу /etc/passwd на рисунку 4.25.

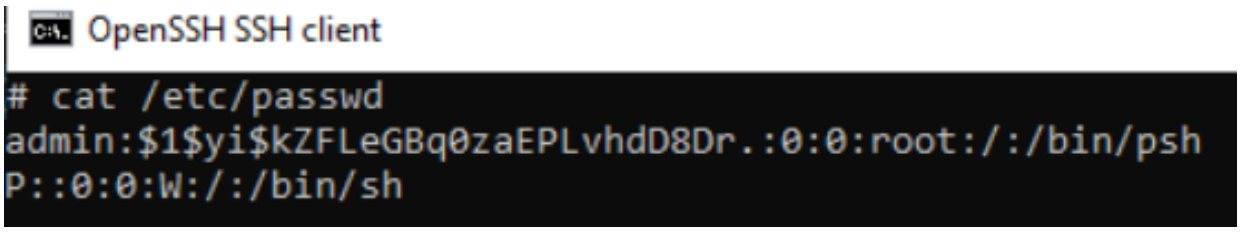


Рис. 4.25 На рисунку відображаються логін і відповідний хеш-пароль девайсу

Отже, була отримана інформація за девайсом, яку, я, та інші користуачі не повинні знати, вміст "/etc/passwd", завжди є паролем аккаунта головного адміну.

Так, якщо зловмисник отримує доступ до файлу "/etc/passwd" або аналогічного файлу, де зберігаються облікові записи користувачів з хешами їх паролів, він може використати цю інформацію для отримання доступу до системи або внесення змін до існуючих облікових записів, включаючи обліковий запис адміністратора веб-порталу камери. Один з методів, яким можна скористатися зловмисник, це редагування цього файлу, або його аналогічного, для створення нових облікових записів або зміни існуючих. Це може дозволити зловмиснику отримати повний доступ до системи або веб-порталу камери, якщо він успішно отримає доступ до правильних облікових даних. Обліковий запис показано на рис. 4.26.

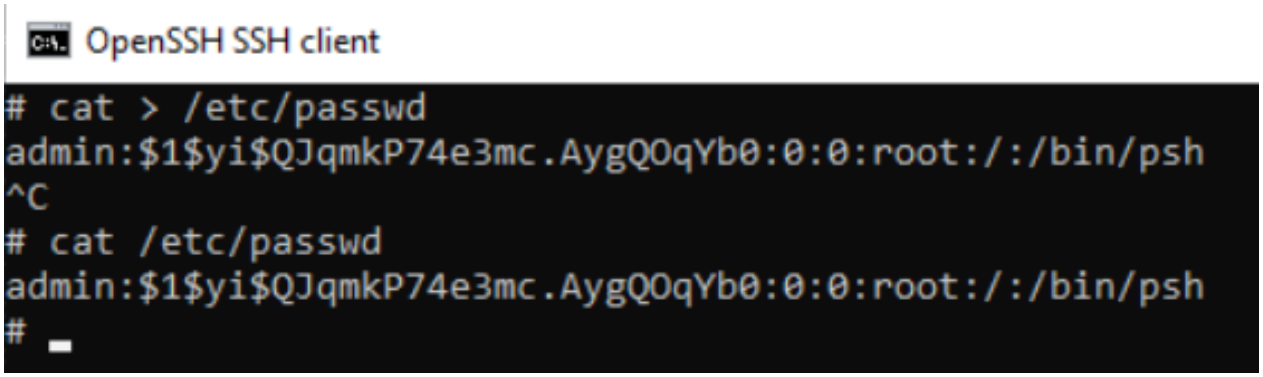


Рис. 4.26 Данні облікового запису

На рис. 4.26 відображається хеш пароля за допомогою алгоритму хешування MD5Crypt. MD5 вже оголошено криптографічно зламаним через свою вразливість до хеш-колізійних атак. Md5crypt в основному використовувався в дистрибутивах Unix і Linux для захисту паролів. Його використання поширюється на інші системи, які потребують безпечного зберігання паролів і перевірки. md5crypt використовує алгоритм хешування MD5, але вводить численні ітерації (за замовчуванням 1000 разів) і сіль процесу хешування. Це значно збільшує складність злому хешів. Використання унікальної солі для кожного пароля є важливою особливістю

md5crypt. Ця сіль заважає зловмисникам ефективно використовувати райдужні таблиці та значно перешкоджає спробам грубої сили.

Таким чином, враховуючи вхідні дані для підбору пароля використовувалася словникова атака з використанням уже згаданого JtR, результати атаки підбору пароля показані на рисунку 4.27.

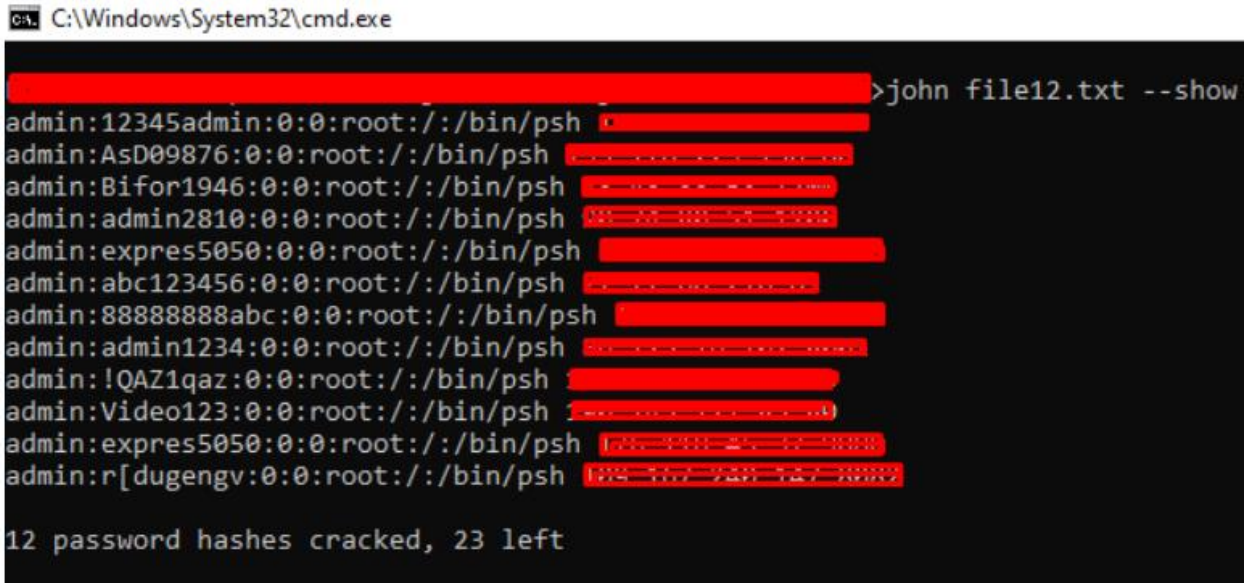


Рис. 4.27 Паролі доступу до камери

З рис. 4.27 можна переглянути вибрані паролі, та їх загальну кількість.

Більшість користувачів дотримуються основних правил встановлення надійного пароля. Використовуючи вразливість віддаленого виконання коду, зловмисник може автоматизувати або виконати зараження системи спостереження, наприклад, за допомогою шкідливого програмного забезпечення Stealer.

Шкідливе програмне забезпечення Stealer є одним з найпоширеніших типів зловмисних програм, що виявлені сьогодні. Мета зловмисників полягає у викраденні якомога більшої кількості особистих даних, починаючи від основної системної інформації і закінчуючи локально збереженими іменами користувачів та паролями.

У цьому випадку шкідливе програмне забезпечення "Stealer" використав для вилучення файлу бази даних віддалених користувачів з усіма обліковими даними, даними автентифікації бездротових мереж, хмарних сервісів (FTP, P2P, Telnet, електронної пошти тощо), топології локальних мереж, відео та аудіозаписів.

Атака може також надати інформацію про план будівлі, цінні предмети всередині та пристрої в мережі за допомогою IP-камер. Якби зловмисники отримали доступ до цієї інформації, це становило б серйозне порушення конфіденційності.

4.2 Побудова безпечної IoT системи

Система IoT включає такі пристрої:
- 3 розумних дверних замки;
- 3 датчики відкриття вікон;
- 2 розумні лампи;
- 3 датчики включення світла;
- 1 базова станція, шлюз.

Для забезпечення зв'язку використовуються наступні протоколи:
- На канальному рівні використовується технологія Wi-Fi для всіх сенсорів.
- На мережевому рівні використовується IPv4 протокол.
- На транспортному рівні підтримуються протоколи TCP та UDP.
- На рівні додатків використовуються протоколи MQTT, Вебсокет

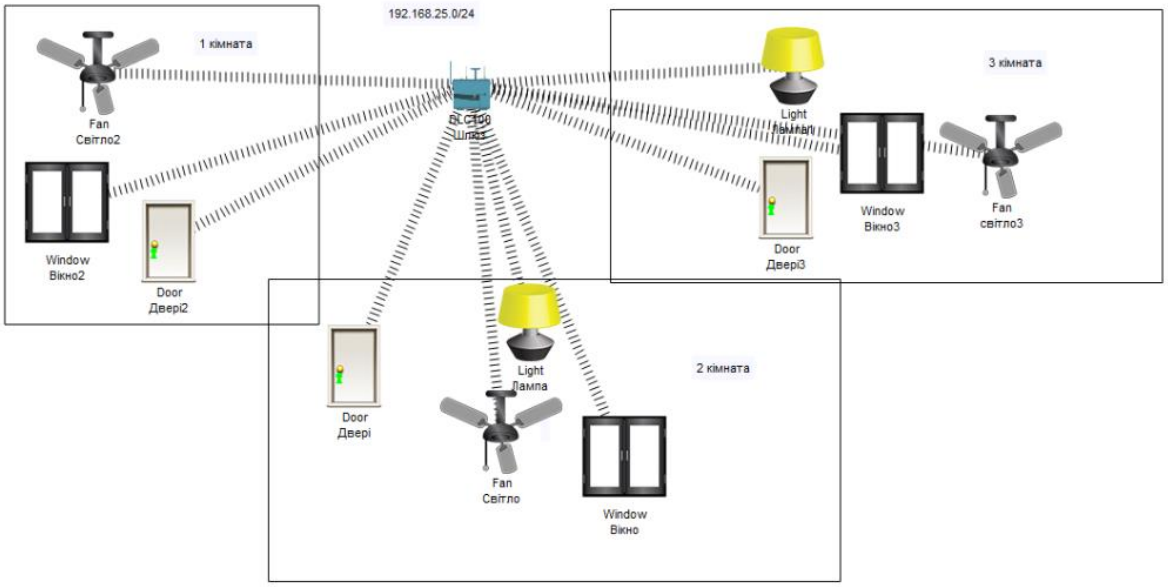


Рис 4.28 Топологія інтернету речей

На рисунку 4.28 представлена топологія IoT системи, яка була розроблена за допомогою PacketTracer. Ця топологія відображає підключення всіх сенсорів до мережі за допомогою шлюзу, який відповідає за маршрутизацію даних і їх передачу.

Мережа Інтернету речей ізольована і має адресне простір 192.168.25.0/24. У системі використовується модель запит-відповідь та API-зв'язок на основі REST і WebSocket.

Щодо забезпечення безпеки, ми вибрали використання TLS/SSL аутентифікації поверх MQTT (див. рисунки 4.29-4.30).

У наведеному підході до безпеки використовуємо метод аутентифікації, який посилюю за допомогою TLS/SSL аутентифікації. На рівні додатків, де застосовується протокол MQTT, впроваджую захист SSL/TLS через платформу IBM Watson IoT Platform.

Це програмне забезпечення для системи Інтернету речей призначене для з'єднання сенсорів з хмарою. Платформи IoT розташовані між рівнем сенсорів та додатків. Замість датчика, ініціювати підключення до хмари буде смартфон. Після створення пристрою, завантажуємо додаток на смартфон і пройдемо етап аутентифікації для підключення до платформи.

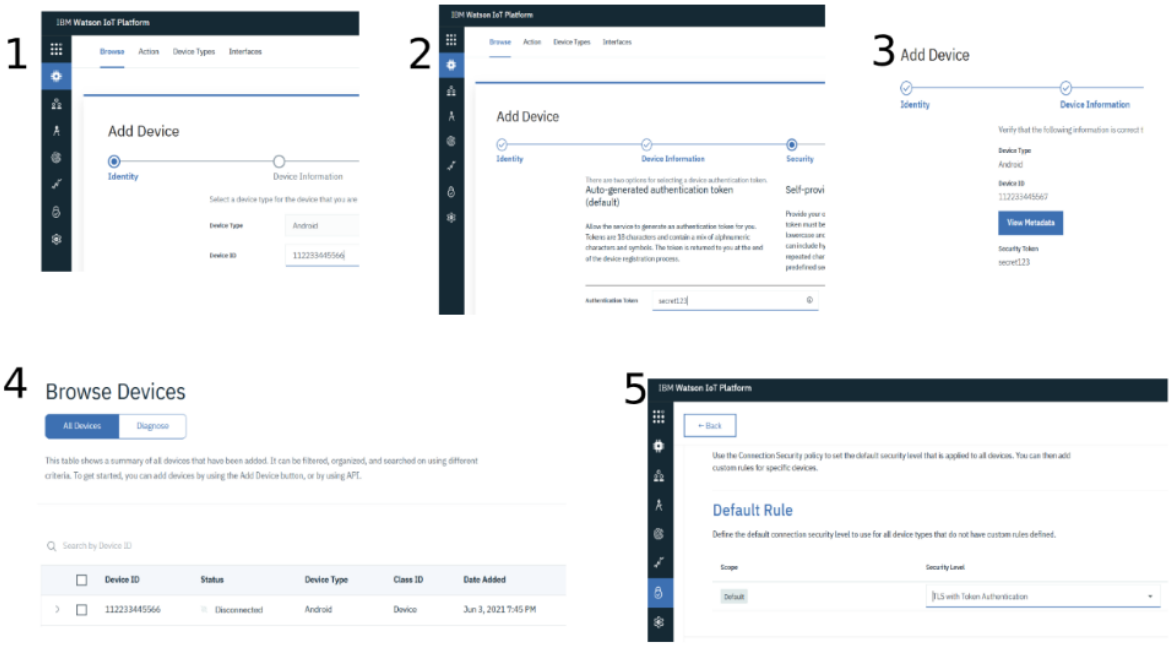


Рис. 4.29 Створення пристрою в IoT-плаформі

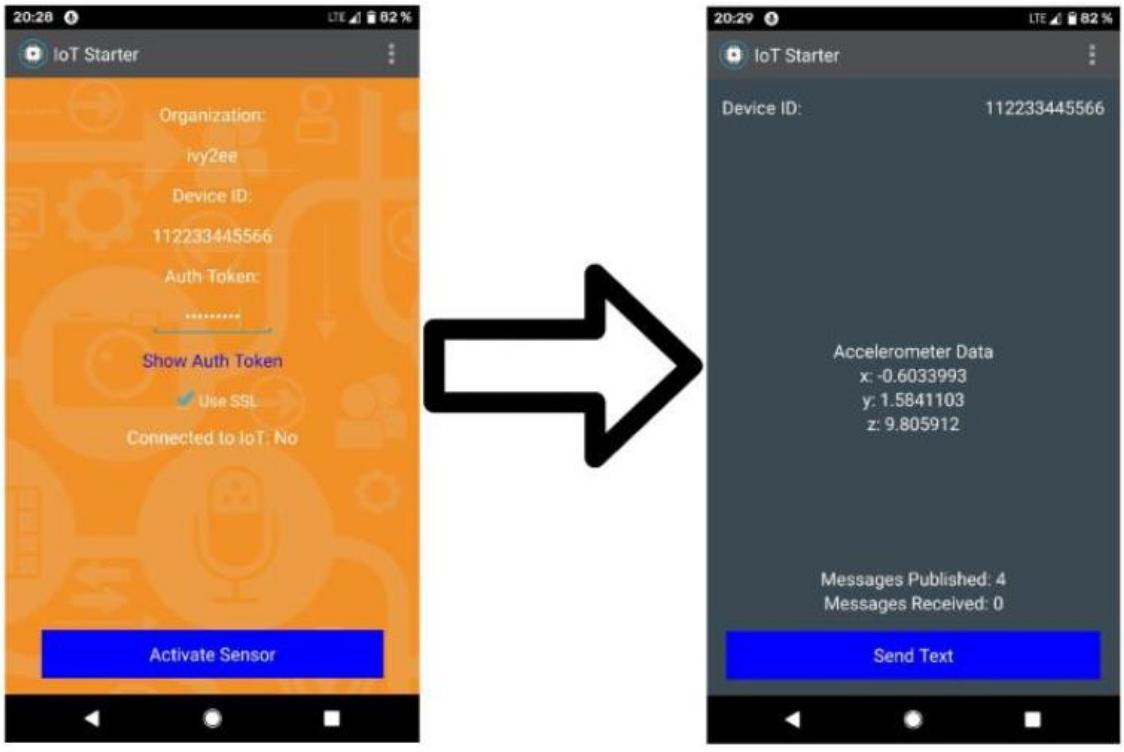


Рис. 4.30 Аутентифікація пристроя та впровадження контролю доступу

Розглянемо створення нової ролі та надамо їй певні права, відредагувавши доступ до шлюза та користувача. Однак, важливо також врахувати потенційні загрози безпеці, пов'язані з оновленням програмного забезпечення. Щоб запобігти можливим атакам, важливо:

1. Забезпечити оновлення програмного забезпечення на всіх пристроях, включаючи шлюз та всі підключені пристрої IoT.

2. Встановити механізми моніторингу та виявлення вразливостей для оперативного реагування на нові загрози.

3. Запровадити строгі правила безпеки доступу, включаючи сильні паролі, механізми аутентифікації та авторизації.

4. Провести навчання персоналу з питань кібербезпеки, щоб уникнути соціального інженерінгу та інших видів атак.

Шляхом цих заходів можна зменшити ризик використання вразливостей в новій версії програмного забезпечення.

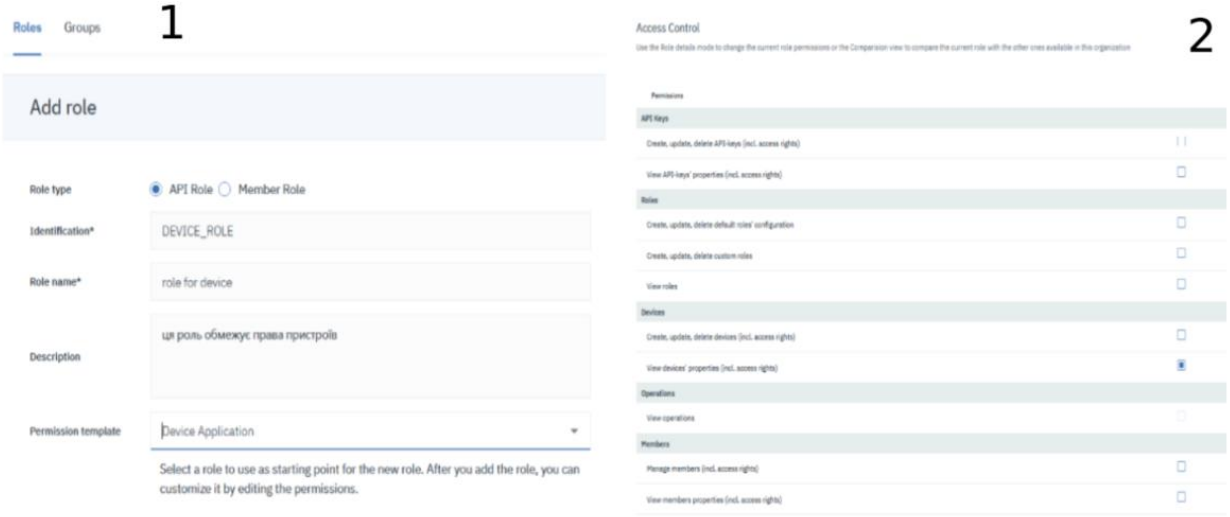


Рис. 4.31 Створення контролю доступу для пристроїв

Впроваджуємо TPM модуль створення ключів для підвищення безпеки обміну інформацією між об'єктами Інтернету речей. (Trusted Platform Module) виявляється оптимальним рішенням з кількох причин:

1. Забезпечення цілісності пристрою: дозволяє зберігати і захищати ключі шифрування від несанкціонованого доступу, забезпечуючи цілісність пристрою та захищаючи дані від зловмисних атак.

2. Робота в безпечному режимі: може працювати в безпечному режимі, що дозволяє зменшити можливість шкоди в разі зараження пристрою шкідливим програмним забезпеченням. Це робить його важливим елементом для забезпечення безпеки в умовах зростаючих загроз кібербезпеці.

3. Встановлення кореня довіри: допомагає встановити корінь довіри для системи, що є основою для побудови надійних систем безпеки, включаючи аутентифікацію та шифрування даних.

Отже, впровадження TPM модуля дозволяє створити надійну і безпечну інфраструктуру для обміну інформацією в системі Інтернету речей, забезпечуючи захист від різноманітних загроз кібербезпеці.

Рис. 4.32 TPM модуль

Основні рівні забезпечення безпеки для системи Інтернету речей (IoT) є критичними для захисту від різноманітних загроз кібербезпеки. Нижче наведено опис та реалізацію запропонованих рішень для кожного рівня безпеки: Забезпечення зв'язку, Безпеку пристроїв на рівні коду та Безпеку при використанні пристроїв

1. Забезпечення зв'язку включає:

- Шифрування трафіку: Використання методу Еліптичної криптографії для шифрування трафіку забезпечує конфіденційність інформації під час передачі через мережу.

- Перевірка автентичності: Впровадження сертифікатів безпеки X.509 дозволяє підтверджувати автентичність пристроїв та забезпечувати безпечний обмін даними.

2. Безпека пристроїв на рівні коду включає:

- Використання бібліотеки OpenSSL для перевірки автентичності та підтвердження виконання необхідного коду пристрою забезпечує безпеку на рівні програмного забезпечення.

3. Безпека при використанні пристроїв включає:

- Впровадження системи розмежування доступу і застосування аналітичної системи безпеки UBA дозволяє виявляти аномальну активність та забезпечує захист від різних загроз.

Додаткові практики з поліпшення безпеки включають:

- Регулярне оновлення системи та встановлення захисного програмного забезпечення.

- Проведення аудитів інфраструктури мережі за допомогою сервісу AWS IoT Device Defender.

- Використання брандмауера для контролю вхідного та вихідного трафіку на пристроях IoT.

- Створення надійних та унікальних паролів з їх регулярною зміною.

- Ізоляція мережі для IoT для підвищення складності доступу зловмисників.

Ці заходи сприяють підвищенню безпеки системи Інтернету речей та зменшують ризик вразливості перед різноманітними загрозами кібербезпеки.

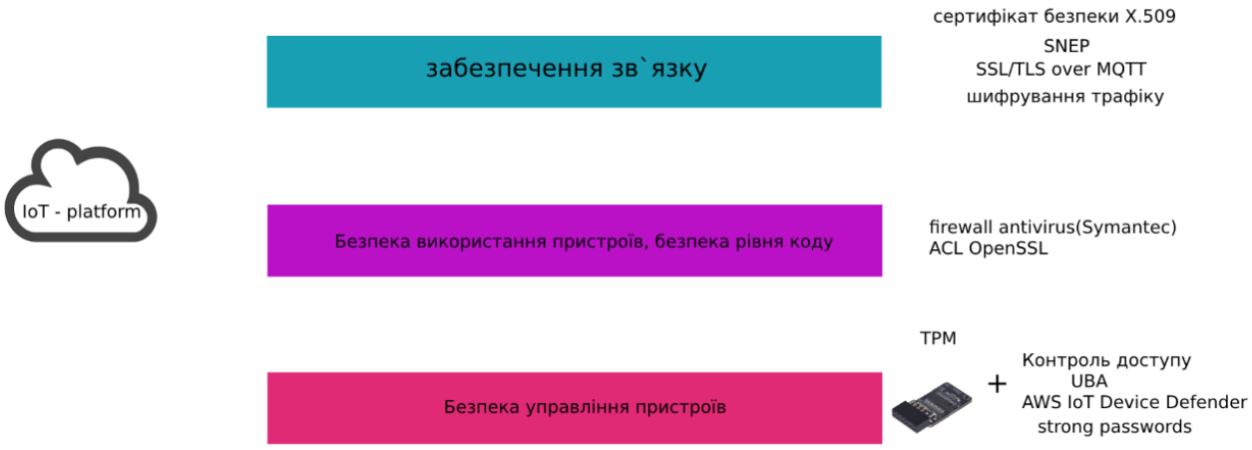


Рис. 4.33 Система методів безпеки для спроектованої системи IoT

Отже, найпростіший спосіб оцінити рівень системного ризику – перевірка можливості отримати доступ до веб-сторінки пристрою без додаткових змін мережі.

ВИСНОВКИ

У ході даної дипломної роботи було проведено аналіз вразливостей пристроїв Інтернету речей (IoT) та розроблено рекомендації щодо підвищення безпеки в мережі IoT. Створена система Інтернету речей має велике значення з точки зору безпеки. Пропонуються методи захисту для забезпечення безпеки цієї системи. Рекомендації щодо впровадження цих методів безпеки також надаються з метою підвищення захищеності системи. Нижче наведені основні висновки з проведеного дослідження:

– Уразливості пристроїв Інтернету речей: виявлено, що пристрої Інтернету речей мають низку поширених уразливостей, таких як слабкі паролі, відсутність оновлень програмного забезпечення та недостатній захист мережевого трафіку. Ці вразливості створюють серйозні ризики для інформаційної безпеки та конфіденційності користувачів.

– Методи оцінки безпеки. Для оцінки безпеки пристроїв IoT застосовувалися різні методи, такі як сканування вразливостей мережі, аналіз трафіку, тестування на проникнення та аудит безпеки програмного забезпечення. Ці методи дозволили виявити потенційні ризики безпеки та визначити шляхи їх вирішення.

– Рекомендації щодо підвищення безпеки: На основі аналізу розроблено рекомендації щодо підвищення безпеки пристроїв IoT. До них належать встановлення регулярних оновлень програмного забезпечення, впровадження суворої автентифікації та авторизації, використання заходів безпеки мережі та навчання користувачів правилам кібербезпеки.

– Практична частина: у практичній частині були обрані конкретні пристрої IoT для оцінки їх безпеки. Проведено аналіз вразливостей, розроблено та реалізовано план підвищення їх безпеки. Результати практичного дослідження підтвердили важливість застосування рекомендацій для підвищення безпеки.

Загальний висновок полягає в тому, що безпека пристроїв IoT є надзвичайно важливою проблемою, яка потребує уваги та системних заходів для забезпечення безпеки користувачів та їхніх даних. Ретельна оцінка вразливостей, розробка та впровадження ефективних заходів безпеки є ключовими кроками у розвитку IT-індустрії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Мазепа А. Д. Безпечна автентифікація до веб-додатку з використанням JWT та browser fingerprinting, матеріали XXII міжнародного молодіжного форуму "Радіоелектроніка та молодь

[2] Тарасов А. С. Проблеми захисту персональних даних в комп'ютерних системах від шкідливого програмного забезпечення stealer

[3] Мазепа А. Д. Розуміння та захист від атаки DNS rebinding, матеріали XXII міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті".

[4] The Internet of Things - https://www.networkcultures.org

[5] Наукове дослідження Інтернету речей - https://json.tv/

[7] Що таке Шодан? - https://help.shodan.io/the-basics/what-is-shodan.

[8] Shodan - https://money.cnn.com/

[9] Dahua IP Camera 3.200.0001.6 access control - https://vuldb.com/

[10] John the Ripper - https://ru.wikipedia.org/

[11] Vulnerability CVE-2021-33045 - https://www.cvedetails.com/

[12] Vulnerability CVE-2021-36260 - https://www.cvedetails.com/

[13] Quantitative Risk Analysis - https://sansorg.egnyte.com/

[14] TechTarget Launches IoTAgenda.com to Help Enterprises Better Leverage the Internet of Things - https://www.techtarget.com/

[15] Awesome IoT Hacks - https://github.com/

[16] Attackers Exploit Flaw that Could Impact Millions of Routers, IoT Devices - https://www.esecurityplanet.com/

[17] Search Engine for the Internet of Everything - https://www.shodan.io/

[18] Кібербезпека в гіперз'єднаному світі: захист пристроїв Інтернету речей і розумних будинків - https://hackyourmom.com/

[19] Безпека пристроїв інтернету речей http://www.studfiles.ru/

[20] Міжнародна конференція «Виклики та реалії IT-простору: інженерія програмного забезпечення та кібербезпека» - shttps://knute.edu.ua/

[21] Основи цифрової економіки - http://dspace.wunu.edu.ua/

[22] Administrative Law and Process - https://applaw.net/

[23] Актуальність безпеки інтернет речей - https://openarchive.nure.ua/

[24] Ефективна система кібербезпеки - https://corewin.ua/

[25] Develop custom web services and mobile applications - https://stfalcon.com/

ПРЕЗЕНТАЦІЯ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА

НА ТЕМУ:

«ОЦІНКА ВРАЗЛИВОСТЕЙ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ І НАДАННЯ РЕКОМЕНДАЦІЙ З БЕЗПЕКИ ІНФОРМАЦІЇ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: студент групи ІСД-41
Хитрін Артем
Науковий керівник роботи:
Каграманова Ю.К.

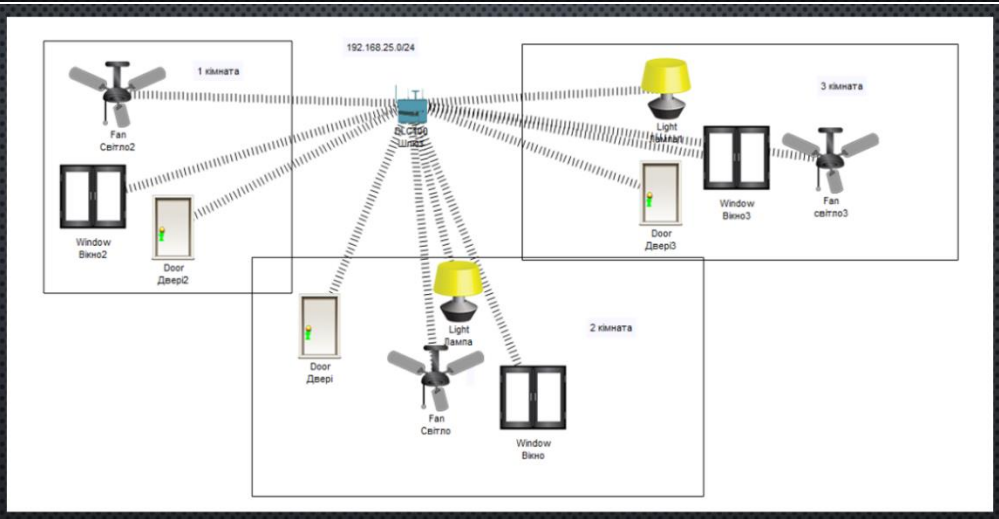
Київ - 2024

- ***Актуальність теми:*** **Збільшення потенційних загроз для кібербезпеки та конфіденційності даних**
- ***Наукова новизна:*** **розробка системи забезпечення безпеки даних і пристроїв у системі інтернету речей**
- ***Об`єкт дослідження:*** **Інформаційна безпека інтернету речей**
- ***Предмет дослідження:*** **Методи та способи захисту системи інтернету речей**
- ***Мета дослідження:*** **Аналіз та розробка методів безпеки**
- ***Завдання дослідження:*** **Оцінка вразливостей пристроїв інтернету речей**
  - **Аналіз та методи оцінки безпеки IoT-пристроїв**
  - **Рекомендації з підвищення безпеки IoT**
  - **Оцінка вразливості пристроїв IoT**

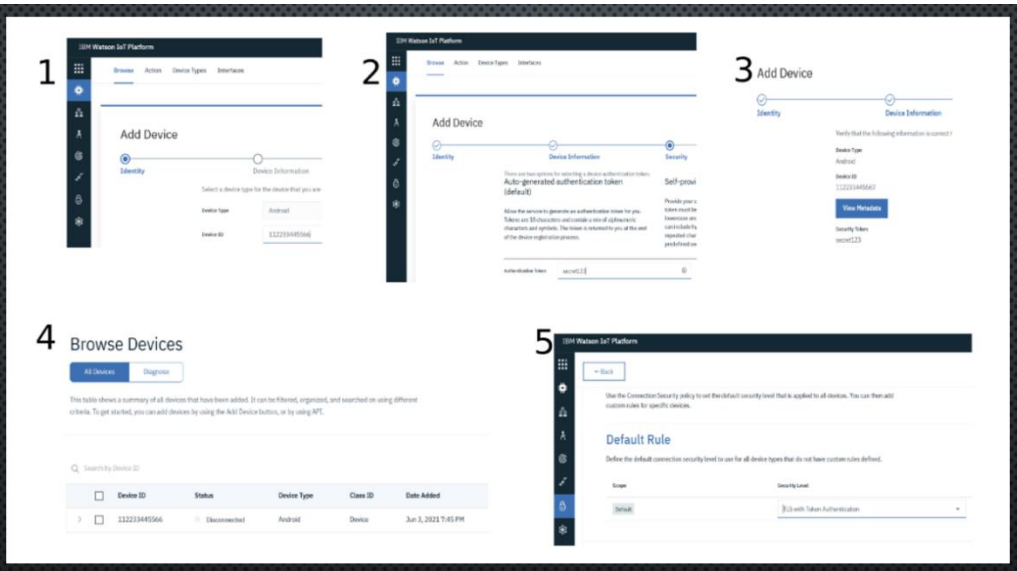
2

ТЕОРІЯ

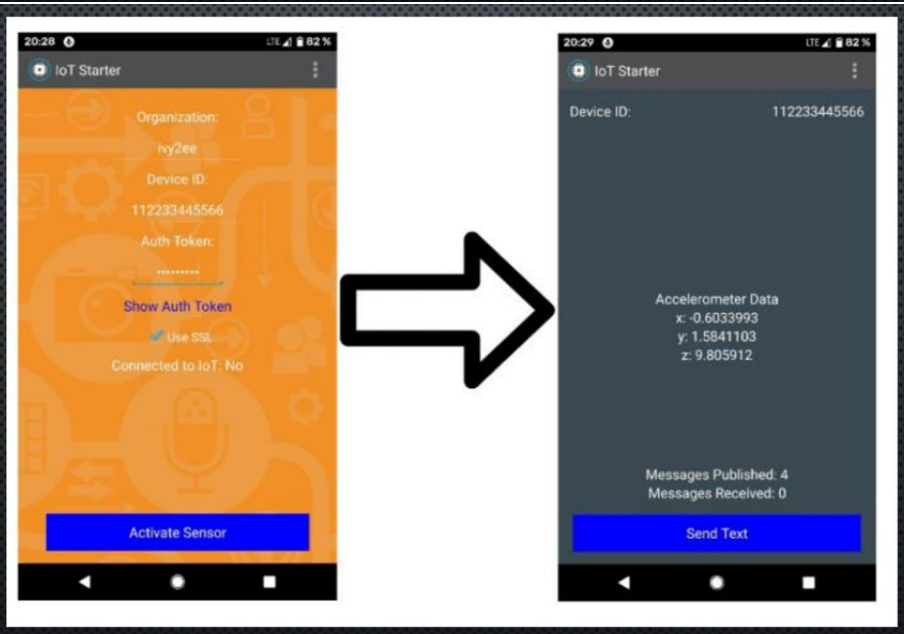
- Використання пристроїв IoT у сучасному світі
- Необхідність розгляду зростаючої кількості взломів
- Проблеми безпеки в сфері Інтернету речей
- Дослідження пристроїв Інтернету речей



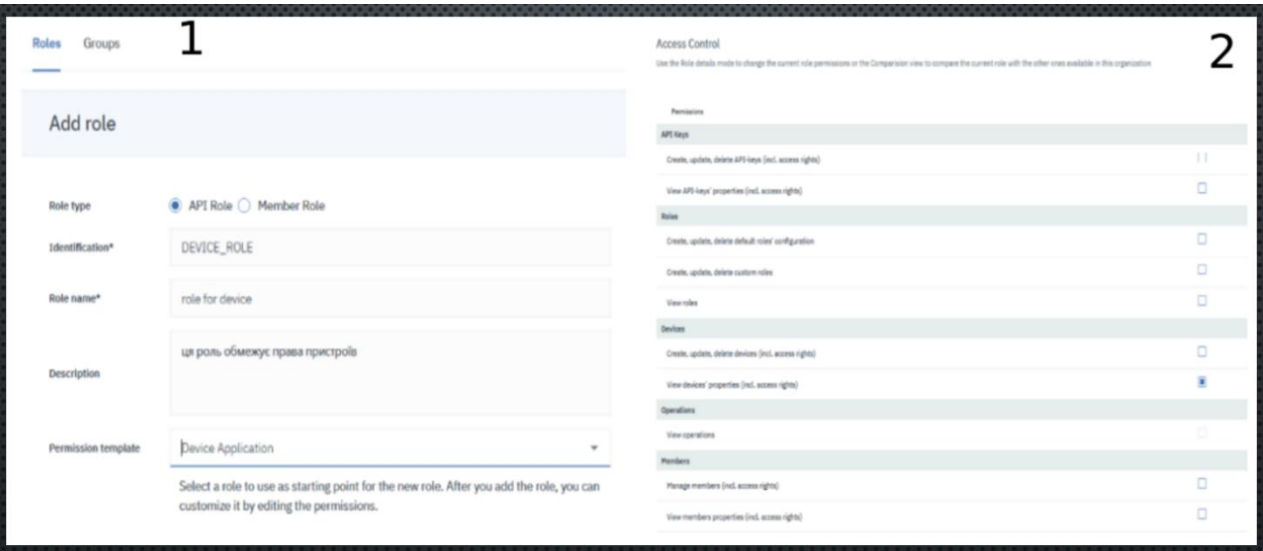
ТОПОЛОГІЯ IOT СИСТЕМИ, ЯКА БУЛА РОЗРОБЛЕНА ЗА ДОПОМОГОЮ PACKETTRACER



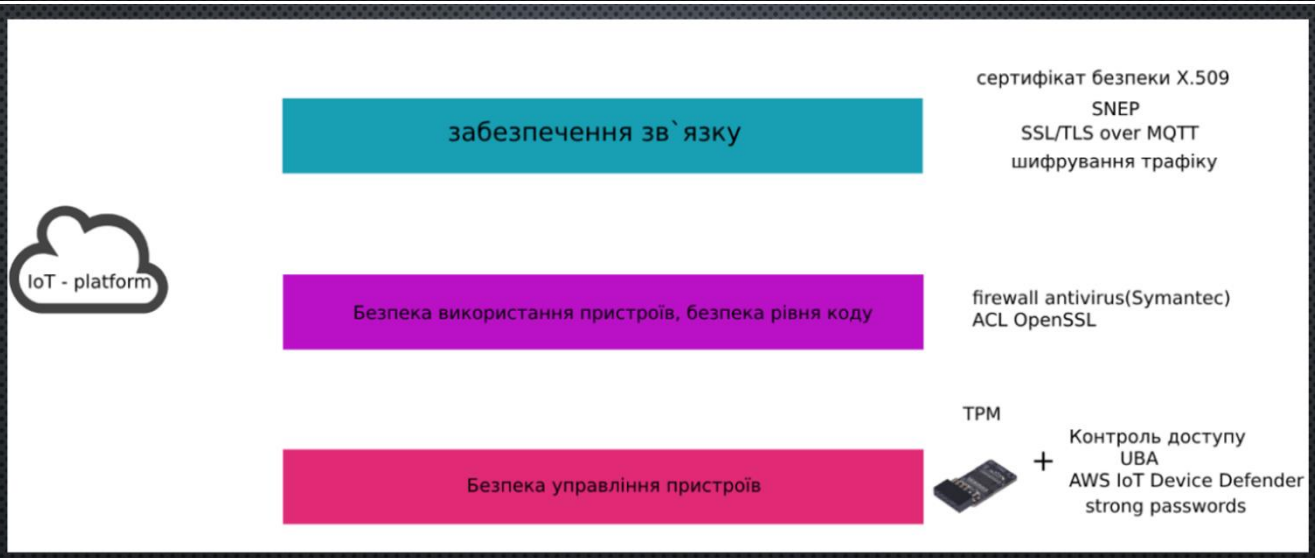
СТВОРЕННЯ ПРИСТРОЮ В IOT-ПЛАФОРМІ. ПІСЛЯ СТВОРЕННЯ, ЗАВАНТАЖУЄМО ДОДАТОК НА СМАРТФОН



АУТЕНТИФІКАЦІЯ ПРИСТРОЮ ТА ВПРОВАДЖЕННЯ КОНТРОЛЮ ДОСТУПУ



СТВОРЕННЯ КОНТРОЛЮ ДОСТУПУ ДЛЯ ПРИСТРОЇВ



СИСТЕМА МЕТОДІВ БЕЗПЕКИ ДЛЯ СПРОЕКТОВАНОЇ СИСТЕМИ IOT

ВИСНОВКИ

Зроблено дослідження щодо обходу методів забезпечення інформаційної безпеки в пристроях мережі Інтернету речей. Мета роботи була досягнута, тобто було зроблено безпечну IOT систему враховуючи усі можливі вразливості. Проведено аналіз проблем та загроз інформаційної безпеки Інтернету речей. Встановлено актуальні та найважливіші загрози безпеки пристроїв IoT в мережах, відповідно надано основні рекомендації. При дослідженні було емпірично доведено актуальність методів забезпечення інформаційної безпеки в мережах Інтернету речей.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Попередні результати роботи були апробовані на V Міжнародній науково-технічній конференції "Сучасний стан та перспективи IOT", яка проходила 18 квітня 2024 року. Тези на тему "Пристрої IOT та захист" та "Захист пристроїв IOT" було опубліковано у збірнику, присвяченому цій конференції

Дякую за увагу!