Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Тестування на проникнення IoT−пристроїв"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Микитюк Т.В.
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Микитюку Тарасу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Тестування на проникнення IoT пристроїв

Керівник роботи Лечаченко Тарас Анатолійович, доктор філософії., старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 21.12.2024

3. Вихідні дані до роботи Інтернет джерела, наукові джерела, OWASP, ENISA.

4. Зміст роботи (перелік питань, які потрібно розробити)
Огляд Internet of Things (IoT); Огляд загроз і вразливостей для IoT пристроїв; Огляд OWASP IoT TOP 10; Методи захисту IoT пристроїв на етапі розробки; співвідношення OWASP IoT TOP 10 і рекомендацій ENISA; Інструменти для ідентифікації вразливостей у IoT-пристроях; ідентифікація пристроїв у мережі; Методологія тестування мережі; Інвентаризація пристроїв та збір інформації; Короткий аналіз результатів інвентаризації; Збір інформації про сервіси; Аналіз потенційних загроз; Аналіз можливих наслідків атак; Охорона праці та безпека в надзвичайних ситуаціях; Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема дипломної роботи та її актуальність; Мета і завдання дослідження; Об'єкт і предмет дослідження; Наукова новизна роботи; Практичне значення отриманих результатів; Актуальні загрози IoT-пристроїв; Огляд OWASP IoT Top 10; Методологія дослідження; Результати сканування пристроїв у домашній мережі; Компрометація IP-камери; Недоліки у захисті IoT-пристроїв; Рекомендації з підвищення безпеки IoT-пристроїв; Практичні приклади з відомих інцидентів; Висновки дипломної роботи;

Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.09	
2.	Підбір наукових джерел про тестування IoT-пристроїв	25.09-29.09	
3.	Аналіз загроз і вразливостей IoT-середовищ за OWASP IoT Top 10	01.10-05.10	
4.	Огляд інструментів для сканування мережі	06.10 – 10.10	
5.	Розробка методики тестування безпеки IoT-пристроїв	11.10 – 15.10	
6.	Сканування мережі та ідентифікації пристроїв	16.10 – 20.10	
7.	Проведення аналізу результатів сканування Nmap	21.10 – 24.10	
8.	Проведення аналізу результатів сканування Angry IP Scanner	25.10 – 28.10	
9.	Порівняльний аналіз результатів сканування двома інструментами	29.10 – 31.10	
10.	Дослідження інцидентів з залученням IoT-пристроїв	01.11 – 05.11	
11.	Аналіз виявлених вразливостей та розробка рекомендацій для підвищення їх безпеки	06.11 – 10.11	
12.	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»	11.11 – 15.11	
13.	Підготовка звіту та оформлення кваліфікаційної роботи	16.11 – 25.11	
14.	Нормоконтроль	16.12	
15.	Перевірка на плагіат	17.12	
16.	Попередній захист кваліфікаційної роботи	25.12-26.12	
17.	Захист кваліфікаційної роботи	27.12	

Студент _____ Микитюк Т.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тестування безпеки IoT-пристроїв у мережах домашнього використання // Кваліфікаційна робота магістра // Микитюк Тарас Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2024 // с. – 85, рис. – 3, табл. – 3, бібліогр. – 35, додат – 1.

Ключові слова**:** Інтернет речей (IoT), тестування на проникнення, Mirai, OWASP IoT Top 10, NMAP, Shodan, Metasploit, Burp Suite.

У магістерській роботі досліджено методи тестування безпеки IoT-пристроїв у мережах домашнього використання. Проведено аналіз загроз для IoT-середовищ та актуальних вразливостей згідно з OWASP IoT Top 10. Розроблено методику тестування IoT-пристроїв із використанням інструментів NMAP, Shodan, Metasploit та Burp Suite. Проведено дослідження захищеності IoT пристроїв у домашній мережі. Запропоновано рекомендації щодо підвищення безпеки домашніх IoT-мереж на основі виявлених вразливостей та аналізу потенційних загроз.

ABSTRACT

Security Testing of IoT Devices in Home Networks // Master's Qualification Thesis // Mykytiuk Taras Volodymyrovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, Group SBm-62 // Ternopil, 2024 // pp. – 85, figs. – 3, tables – 3, references – 35, added – 1.

Keywords: Internet of Things (IoT), penetration testing, Mirai, OWASP IoT Top 10, NMAP, Shodan, Metasploit, Burp Suite.

The master's thesis explores methods for security testing of IoT devices in home networks. An analysis of threats to IoT environments and current vulnerabilities is conducted based on the OWASP IoT Top 10. A methodology for testing IoT devices using tools such as NMAP, Shodan, Metasploit, and Burp Suite has been developed. The security of IoT devices within a home network has been examined. Recommendations have been proposed to improve the security of home IoT networks based on identified vulnerabilities and analysis of potential threats.

ЗМІСТ

ВСТУП

Дослідження безпеки IoT-пристроїв через методи penetration testing є надзвичайно актуальним у сучасному світі, де технології стають дедалі більш інтегрованими в повсякденне життя. З розвитком концепції "інтернету речей" мільярди пристроїв — від розумних лампочок до медичних пристроїв — підключаються до мереж, створюючи нові можливості для ефективного управління ресурсами та підвищення комфорту. Проте з цим зростає і кількість загроз.

Відкритість IoT-систем робить їх вразливими до кіберзагроз, оскільки такі пристрої часто не мають належних механізмів захисту. Хакери можуть використовувати слабкі місця в безпеці для отримання доступу до особистих даних або навіть для контролю над критично важливими системами. Інциденти, пов'язані з несанкціонованим доступом до розумних будинків, автомобілів чи промислових мереж, свідчать про необхідність розробки ефективних методів захисту IoT.

Penetration testing — це ключовий інструмент для виявлення вразливостей в таких системах. Він дозволяє імітувати реальні атаки, щоб виявити слабкі місця та розробити відповідні контрзаходи до того, як зловмисники скористаються ними. Особливу увагу варто звернути на те, що IoT-пристрої відрізняються обмеженими ресурсами, що ускладнює їхнє ефективне захищення традиційними засобами, такими як антивіруси або складні шифрувальні алгоритми. Зважаючи на все це, дослідження у цій сфері допоможе не лише виявити потенційні загрози, але й запропонувати оптимальні рішення для захисту цих пристроїв, що стають невід'ємною частиною нашого життя.

Метою цієї роботи є дослідження безпеки пристроїв Інтернету речей (IoT) з використанням методів penetration testing для виявлення вразливостей та розробки практичних рекомендацій щодо їх захисту. У сучасному цифровому середовищі безпека IoT стає ключовим викликом, адже з кожним новим підключеним пристроєм зростає ризик несанкціонованого доступу до даних або

систем. Тому ця робота спрямована на детальний аналіз загроз, які стоять перед IoT-пристроями, та на застосування методик тестування проникнення для виявлення слабких місць у їхній архітектурі.

Завдання роботи полягають у наступному: провести огляд існуючих методів забезпечення безпеки IoT, дослідити сучасні інструменти для penetration testing, здійснити практичне тестування на прикладі конкретних IoT-пристроїв, проаналізувати отримані результати та надати рекомендації для підвищення рівня безпеки IoT-систем. Важливо також дослідити особливості, що відрізняють IoT від традиційних IT-систем, зокрема їхні обмежені ресурси та складність інтеграції захисних механізмів.

Об’єктом дослідження є пристрої Інтернету речей (IoT), які підключені до домашньої мережі користувача. Вони включають в себе декілька IoT пристроїв від айпі камер до розумного пилососа, що представляють типові пристрої, широко використовувані в сучасних розумних будинках. Крім того, об’єктом дослідження можуть стати додаткові пристрої або сервери, які будуть створені у вигляді віртуальних машин, що дозволить розширити спектр аналізованих систем.

Предметом дослідження є процеси виявлення вразливостей у безпеці цих IoT-пристроїв. Це включає аналіз методів тестування на проникнення, застосованих до зазначених пристроїв, вивчення їх вразливостей, способів їх експлуатації та подальшої розробки рекомендацій щодо покращення безпеки.

У дослідженні будуть застосовані як теоретичні, так і практичні методи. Теоретична частина передбачає аналіз літературних джерел та наукових публікацій, присвячених проблемам безпеки IoT-пристроїв та методам їх тестування на проникнення. Особлива увага буде приділена вивченню підходів до виявлення вразливостей у ресурсно-обмежених системах, таких як IoT, та огляду інструментів penetration testing, зокрема для аналізу мережевої безпеки.

Практичні методи включатимуть проведення penetration testing для конкретних IoT-пристроїв у домашній мережі, таких як IP-камери, розумний пилосос і телевізори. Для цього будуть використані такі інструменти, як Nmap,

та інші програми для мережевого аналізу і тестування. Таким чином, комбінація теоретичних і практичних методів дозволить отримати повну картину вразливостей IoT-пристроїв і розробити ефективні рекомендації для їхнього захисту.

Структура роботи передбачає три основні розділи: теоретична частина, аналітична частина і практична частина. Спершу буде розглянуто теоретичну частину в якій буде здійснено огляд існуючих наукових публікацій та досліджень, що стосуються загроз і викликів безпеки IoT-пристроїв. Після цього перейдемо до аналітичної частини, де буде висвітлено методологічні підходи до тестування на проникнення для систем IoT, зокрема вибір інструментів та проведення атак. Останнім етапом буде практична частина, в цій частині буде проведено практичне тестування IoT пристроїв у мережі. Практична частина буде присвячена реальному тестуванню пристроїв у домашній мережі, таких як розумний пилосос, IP-камери та телевізори. Тут детально описуватимуться етапи тестування, виявлені вразливості та рекомендації для підвищення їх безпеки.

Наукова новизна роботи полягає у розробці методології тестування на проникнення IoT-пристроїв у домашніх мережах, що враховує специфіку ресурсно-обмежених пристроїв та поширені типи загроз. У дослідженні детально розглянуто OWASP IoT Top 10 та рекомендації ENISA, які застосовано для аналізу потенційних вразливостей у сучасних IoT-системах. Запропонований підхід включає інвентаризацію пристроїв, сканування портів і сервісів, а також аналіз загроз і можливих наслідків атак. Це забезпечує комплексне теоретичне тестування на проникнення без проведення реального пентесту, що є оптимальним рішенням для умов, де практичне тестування обмежене

Практичне значення дослідження полягає у можливості використання запропонованої методології для оцінки безпеки IoT-пристроїв у домашніх мережах. Результати роботи дозволяють ідентифікувати поширені вразливості, такі як незахищені сервіси, відкриті порти та неправильні конфігурації пристроїв. На основі аналізу загроз розроблено рекомендації для підвищення безпеки IoT-систем, які можуть бути корисними як для користувачів домашніх

мереж, так і для фахівців з кібербезпеки. Запропонований підхід допоможе вчасно виявляти потенційні загрози та мінімізувати ризики несанкціонованого доступу, витоку даних та інших атак на IoT-пристрої.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічній конференції «Інформаційні моделі, системи та технології.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1. ІОТ-ПРИСТРОЇ ЯК НОВІ ВЕКТОРИ ДЛЯ АТАК

1.1. Огляд Internet of Things (IoT)

Інтернет речей(IoT) – це мережа взаємопов’язаних між собою пристроїв, які спілкуються і обмінюються даними між собою і хмарою. Зазвичай такі пристрої оснащені датчиками, сенсорами, операційною системою та іншими компонентами для забезпечення роботи.

Спектр застосування цих пристроїв неможливо переоцінити, вони охоплюють все: від простих побутових пристроїв, таких як розумні пилососи чи холодильники, до складних промислових систем на заводах – спектр застосування IoT постійно розширюється. З кожним роком потреба у IoT пристроях зростає, адже ці пристрої допомагають автоматизувати рутинні процеси, зменшувати витрати і підвищувати ефективність бізнесу. В недалекому минулому можливо ніхто б і не подумав що ці пристрої будуть мати такий великий вплив на повсякденне життя, але зараз ми бачимо що IoT пристрої використовуються навіть у медицині.

Щороку кількість таких пристроїв зростає в геометричній прогресії. Технологічні компанії та дослідницькі організації активно працюють над впровадженням IoT у різні галузі. Наприклад, у сфері охорони здоров'я пристрої IoT вже стали невід'ємною частиною діагностики та лікування. Один із яскравих прикладів – це проєкт Neuralink, розробкою якого займається компанія відомого американського бізнесмена і винахідника Ілона Маска, який розробляється з метою інтеграції технологій безпосередньо в людський мозок. Уявіть собі систему, яка зчитує мозкові імпульси, обробляє їх і передає сигнали іншим пристроям або безпосередньо у хмару для подальшого аналізу. Декілька років тому це була просто наукова фантастика, а тепер це технологія, що може вивести медицину та реабілітацію на новий рівень, особливо для людей з обмеженими можливостями.

Крім медицини, IoT також стає все більш популярним у сільському господарстві, де використовуються системи автоматизованого поливу або розумні сенсори для контролю за станом ґрунту і врожаю. Ці технології допомагають фермерам ефективніше використовувати ресурси і прогнозувати врожайність, тим самим ефективно знижуючи вплив несприятливих факторів.

Таким чином, IoT-пристрої поступово перетворюються на незамінний елемент як у повсякденному житті, так і в різних галузях економіки. Важливість цих технологій продовжує зростати, і вони стають фундаментом для подальших технологічних інновацій. Проте зі зростанням їх використання постає також питання безпеки, адже кожен новий пристрій у мережі — це потенційна точка входу для зловмисників. З огляду на це, важливість досліджень у сфері безпеки IoT та розробки нових методів захисту не можна переоцінити, адже він ступені захищеності цих пристроїв може залежати не лише ефективність ведення бізнесу, повсякденне життя людей, а також життя і здоров’я певних людей.

1.2. Огляд загроз і вразливостей IoT пристроїв

З розвитком Інтернету речей світ відкрив для себе низку технічних можливостей, де дуже багато пристроїв підключаються до глобальної мережі та взаємодіють один з одним створюючи складну систему. Від розумних будинків до промислових IoT систем, від розумних пилососів і до складних медичних систем, ці технології стали невід'ємною частиною нашого повсякденного життя і мають величезний вплив на різні сфери життя. В той же час, разом із стрімким розвитком цих пристроїв, постають серйозні питання щодо безпеки цих пристроїв, що стає головною темою обговорень у сучасному цифровому просторі.

Інтернет речей забезпечують значне покращення якості життя, автоматизацію рутинних або важких процесів які вимушені були виконувати люди та економію часу. Разом з великою силою – приходить велика відповідальність, разом з перевагами які надають IoT пристрої збільшується і

кількість загроз які можуть стати серйозною проблемою як для окремих користувачів так і для різного розміру бізнесу. Особливо небезпечними є вразливості IoT пристроїв інтегрованих у критичну інфраструктуру: від медичних приладів що підтримують життя і здоров'я пацієнтів до промислових систем підприємств які я важливою частиною економіки країни. Кожен новий пристрій у системі збільшує ризик несанкціонованого доступу до мережі чи атак на інфраструктуру компанії.

Не буде перебільшенням сказати, що одна з основних причин низької захищеності IoT пристроїв полягає у стрімкому розвитку технології, настільки швидкому і невпинному що розвиток безпеки просто не встигає за ним і часто відходить на другий план. Більшість цих пристроїв створюються з акцентом на зручність, функціональність і дешевизну, для задоволення потреб користувачів. В зв'язку з цим створюється новий ландшафт загроз з мільйонами нових потенційних векторів для атак для зловмисників які не пройдуть повз легкої здобичі.

Ще одним викликом для спеціаліста з кібербезпеки це кількість пристроїв які потребують захисту, оскільки більшість пристроїв мають різну апаратну та програмну архітектуру це часто не дозволяє впроваджувати ефективні методи захисту. На додачу до цього, переважно такі пристрої мають обмежені ресурси (мала кількість пам'яті або недостатня обчислювальна потужність процесора), що унеможливлює використання традиційних механізмів безпеки, таких як шифрування чи антивірусне програмне забезпечення. В умовах обмежених ресурсів цих пристроїв, традиційні методи безпеки повинні бути адаптовані до нових умов зі збереженням високого рівня захисту. Крім того, ускладнює контроль за передачею даних і взаємодія IoT пристроїв з хмарними сервісами. Всі перераховані фактори вимагають від вендорів, користувачів і адміністраторів постійної підтримки і роботи направленої на покращення безпеки.

1.3 Огляд OWASP IoT Top 10

Інтернет речей або IoT зробив можливим інноваційні заходи для покращення комунікації потенціальних об’єктів використовуючи інтернет. IoT відіграє важливу роль в повсякденному житті людей, починаючи з розумних будинків і домашніх систем закінчуючи індустріальними системами. Однак, зі збільшенням впровадження IoT пристроїв значно збільшились і проблеми пов’язані з забезпеченням безпечної роботи цих приладів, що потребує значної уваги.

Для ефективного вирішення цих проблем, Open Web Application Security Project (OWASP) визначили топ 10 найголовніших вразливостей які здатні спричинити компрометацію безпеки інтернету речей. Ці вразливості були визначені використовуючи досвід реальних інцидентів які потребують найкращих методів для виявлення і запобігання атак. Список вразливостей OWASP IoT Top 10 був розроблений використовуючи детальну методологію після дослідження реальних інцидентів. В даній роботі буде розглянуто і проаналізовано кожну вразливість, а також досліджено найкращі стратегії запобігання цих вразливостей. На рисунку 1.1 наведено топ 10 вразливостей для IoT пристроїв.

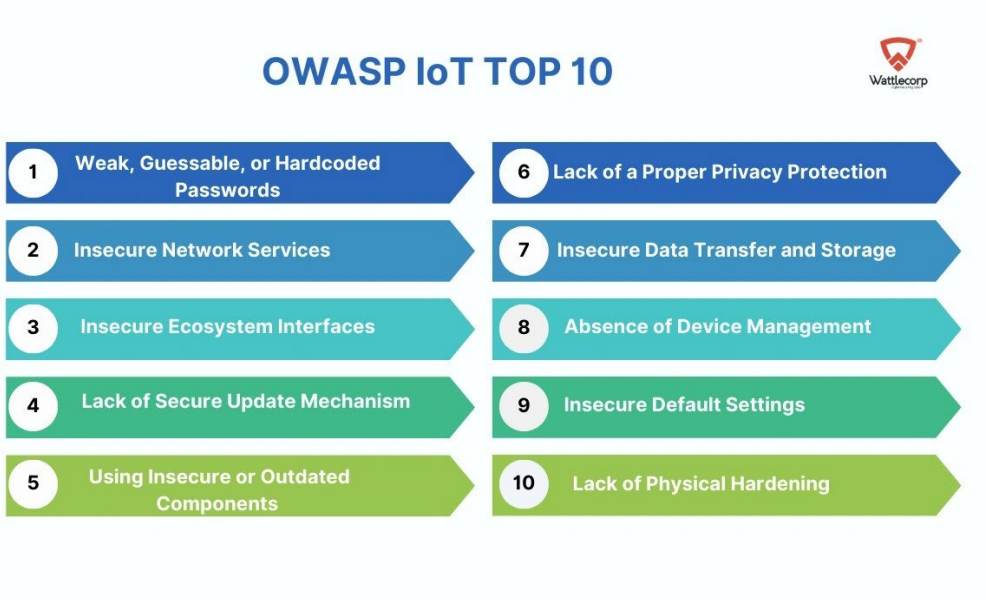

Рисунок 1 – OWASP Top 10 IoT

1.3.1. Weak, guessable or hardcoded passwords

Для адміністрування IoT пристроїв зазвичай використовуються додатки або веб-інтерфейси. Адміністрування включає в себе конфігурацію, управління, оновлення прошивки тощо. Якщо доступ до цих інтерфейсів налаштований неналежним чином, зловмисники можуть з легкістю отримати несанкціонований доступ до цілої системи в якій функціонує скомпрометований IoT девайс, що в свою чергу загрожує порушенням конфіденційності, цілісності і доступності інформації. Забезпечення інформаційної безпеки та захисту конфіденційності, що включає гарантування конфіденційності даних, їх незмінності та доступності, а також запобігання несанкціонованому доступу та маніпуляціям, стають критичними вимогами та заслуговують особливої уваги в контексті Індустрії 5.0[31].

Тестування на проникнення IoT пристроїв показало що більшість скомпрометованих приладів містять логіни і паролі які можна легко вгадати, або перелік стандартних комбінацій логін-пароль знаходиться у вільному доступі. Це створює велику загрозу безпеці, оскільки зловмисники можуть використати цю інформацію для несанкціонованого доступу. Особливо небезпечними є ситуації коли облікові дані зашиті у коді. Це не тільки унеможливлює забезпечення безпеки пристрою шляхом простої зміни стандартних облікових даних при налаштуванні пристрою, але й полегшує зловмисникам процес взлому девайсу. Розробники часто «хардкодять» облікові дані у програмне забезпечення, що і спричиняє проблеми з безпекою.

Впровадження фіксованих паролів є вкрай небезпечним, оскільки навіть якщо зловмисники не можуть використати вразливості механізмів автентифікації, вони можуть використати облікові дані збережені у коді. Це відкриває двері для компрометації пристрою, а можливо й цілої системи, що може завдати великих збитків.

Відтак забезпечення безпеки IoT пристроїв потребує не лише грамотного налаштування додатку або веб-інтерфейсу для керування пристроєм, а й

впровадження складних і унікальних паролів. Розробники повинні уникати використання зашитих у прошивку паролів і замість цього впроваджувати механізми динамічного управління обліковими даними і використовувати унікальні паролі які складно вгадати. Одним з хороших підходів є “User must change password at next logon”, який використовується у Active Directory. Його суть полягає в тому що при першому логіні, користувач повинен змінити стандартний пароль щоб продовжити використовувати продукт. Додаючи до цього вимоги до паролю, такі як мінімальні довжина, використання спец символів, цифр тощо, виходить надійний механізм який забезпечує IoT пристрій складним унікальним паролем. В доповнення до цього, можна імплементувати двохфакторну автентифікацію, що значно підвищить стійкість системи до атак на паролі.

1.3.2. Insecure network services

Insecure network services пов’язане з вразливостями в протоколах безпеки або конфігураціях, такі як незашифровані комунікаційні протоколи, відсутність належних конфігурацій мережевої безпеки та використання застарілих або вразливих компонентів програмного забезпечення. Використовуючи ці вразливості, зловмисник може отримати несанкціонований доступ до пристроїв і мережі, що може спричинити витік чутливої і конфіденційної інформації або використання вразливого пристрою як точка початку атаки на інші системи з якою він пов’язаний. Був випадок коли застарілий сервіс FTP в IoT пристроях використовував зашиті облікові дані, що дозволяло користувачам маніпулювати даними в довільних областях пристрою.

Для зменшення ризиків подібних атак, рекомендується використовувати мережі протоколи які були визнані безпечними, такі як TLS(Transport Layer Security), які забезпечують надійне шифрування даних під час їх передачі. Також, при використані TLS, важливо звернути увагу на те яка версія протоколу використовується і які шифри він підтримує. Окрім того, регулярне оновлення

мережевих сервісів є одним з найважливіших аспектів що допомагає усунити відомі вразливості, що в свою чергу значно підвищить стійкість системи до атак. Не менш важливим кроком є регулярні аудити безпеки вразливостей мережі, цей підхід дозволяє подивитись на безпеку мережі з точки зору зловмисника і вчасно виправити помилки і вразливості якими міг би скористатись зловмисник. До такої активності можна віднести активне сканування мережі використовуючи різні сканери вразливостей, от як Acunetix, Nesus, Nmap та інші. В результаті інтеграції сучасних методів безпеки, постійний моніторинг подій та проактивний менеджмент вразливостей можуть значно знизити ризики пов'язані з ненадійними сервісами IoT, створюючи тим самим більш захищене середовище для пристроїв і користувачів.

1.3.3. Insecure Ecosystem Interfaces

Insecure Ecosystem Interfaces, під цим визначенням мається на увазі ненадійні інтерфейси між різними компонентами у екосистемі IoT. Більшість IoT пристроїв мають веб інтерфейси або мобільні додатки для керування пристроєм або групою пристроїв підключених до локальної мережі. Дуже часто вендори IoT пристроїв, нехтують безпекою цих інтерфейсів, ставлячи на перше місце зручність використання і функціонал. Завдяки цьому, зловмисники можуть використовувати ці інтерфейси для отримання несанкціонованого доступу до конфіденційних даних, порушувати доступність до системи IoT, і що не менш важливо здійснювати атаки на інші системи використовуючи ці інтерфейси як точку входу в мережу.

Зі всіх прикладів інтерфейсів для IoT пристроїв, найнебезпечнішим є API, які не потребують авторизації. Це дозволяє зловмисникам генерувати універсальний ідентифікатор користувача та використовувати його для отримання чутливої або конфіденційної інформації про користувачів. Основною проблемою цих інтерфейсів полягає відсутність належних засобів авторизації, що робить їх пріоритетною ціллю для зловмисників.

Для того щоб уникнути проблем описаних вище необхідно впровадити ряд важливих заходів безпеки. В першу чергу, впровадження механізмів контролю доступу – це дозволить обмежити доступ до чутливих API інтерфейсів що захистить критично важливі дані від несанкціонованого доступу. Не менш важливим кроком є впровадження шифрування даних при передачі. Це унеможливить деякі типи атак і значно підвищить систему до взлому. Останнім, але не менш важливим кроком є регулярне оновлення API. Цей крок дозволить усунути відомі вразливості, а також допоможе виправити помилки і інші проблеми. Всі це механізми передбачають регулярне оновлення програмного забезпечення, посилений контроль доступу, безпечне спілкування між пристроями, та шифрування даних щоб унеможливити небажаний витік інформації.

1.3.4. Lack of Secure Update Mechanism

IoT пристрої, з точки зору споживачів або бізнесу, дуже привабливі, оскільки завдяки своїй економічній ефективності, низькому енергоспоживанню і простоті використання приносять велику кількість користі при малій кількості зусиль. Однак, виробники, та й користувачі, часто нехтують безпекою цих пристроїв через необізнаність чи не хотіння убезпечити ці пристрої від взлому. Відсутність механізму для автоматичного, регулярного оновлення програмного забезпечення або прошивки може зробити систему вразливою до атак які мають відомі експлойти розміщені у публічному доступі. Зловмисники не втратять можливість скористатись застарілим програмним забезпеченням для порушення безпеки пристрою, а в подальшому системи. Вразливості в IoT системах, особливо тих які мають критичне значення, як от платіжні системи, можуть нести серйозні наслідки. Для користувачів це втрата контролю над пристроєм, шпигунські програми або програми вимагачі, а для бізнесу це серйозні репутаційні і фінансові втрати.

Для ефективного усунення згаданих вразливостей, виробникам програмного забезпечення для IoT пристроїв варто розглянути можливість впровадження таких механізмів як примусове автоматичне оновлення і анти-ролбек механізми. Ймовірно це може спричинити для деяких користувачів незручності, але в довгостроковій перспективі це рішення допоможе користувачам уникнути численних проблем і фінансових втрат. Застосування цих методів дозволяє вендорам значно підвищити безпеку пристроїв і стійкість системи до атак, що пов’язані з використанням застарілого програмного забезпечення.

1.3.5. Using Insecure or Outdated Components

Раніше вже було розглянуто проблему відсутності механізму автоматичного оновлення програмного забезпечення, з цього випливає ще одна проблема – використання застарілих або ненадійних компонентів. Багато IoT пристроїв створюються з використанням сторонніх компонентів, з одного боку це значно спрощує розробку програмного забезпечення, з іншого це може призвести до появи додаткових вразливостей. Ці компоненти, часто, погано підтримуються або не підтримуються зовсім, що несе за собою погану якісь програмного забезпечення в плані оновлень і погіршує загальну безпеку пристрою. Особливо це стосується виробників які використовують опен-сорс проекти для створення своєї прошивки, що призводить до складного ланцюга постачання який важко відстежувати. Такі компоненти можуть мати вразливості про які знають зловмисники і створювати загрози для безпеки системи. Ці проблеми можна вирішити регулярним оновленням та виправленням помилок в кожному компоненті та програмному забезпеченні. Завдяки цьому наявні проблеми будуть своєчасно виправлені і усунені що дозволить захистити пристрій від несанкціонованого доступу. Також хорошою практикою є використання системи моніторингу яка буде сповіщати про вразливості в компонентах що використовуються в IoT системі. Це дозволить швидко реагувати на нові загрози

пов’язані з використанням небезпечних компонентів і забезпечити своєчасний захист від потенційних атак. Ці два заходи дозволять значно зменшити ризики пов’язані з використанням вразливих компонентів і забезпечити надійни захист системи від потенційних атак.

1.3.6. Lack of Proper Privacy Protection

Більшість IoT пристроїв отримують і зберігають чутливу особисту інформацію, на жаль, дуже часто без достатнього захисту. Це може включати збір даних без згоди користувача, зберігання даних без належних механізмів захисту цих даних, як от шифрування, або обмін даними з третьою стороною без необхідних дозволів. Наприклад, пристрій який призначений для домашньої автоматизації може збирати інформацію яка може спричинити серйозні проблеми якщо буде втрачена, таку як платіжні дані, персональні дані користувачів чи навіть місцезнаходження. Хоча пристрій дозволяє проводити автоматичні платіжні операції, дані якими він оперує можуть передаватись по мережі без шифрування що несе за собою ризик компрометації. Для вирішення цієї проблеми, в першу чергу, пристрій має забезпечувати шифрування даних, будь це передача їх по мережі чи зберігання в локальній базі даних, це допоможе запобігти несанкціонованому доступу до них з метою викрадення. Також існує принцип який називається: «privacy-by-design» - захист конфіденційності інформації на всіх етапах розробки та використання IoT пристроїв. Останнім механізмом який варто використати для захисту конфіденційної інформації є отримання згоди користувача, хоча цей механізм не передбачає як такого захисту даних, але він як мінімум попереджає користувача про ймовірні наслідки використання пристрою і дозволяє йому підготуватись до ймовірних ризиків. Наприклад знаючи що пристрій не використовує шифрування, користувач не буде зберігати в ньому дані витік яких призведе до серйозних наслідків. Застосування комплексу цих заходів дозволить вендорам забезпечити належний рівень захисту даних користувачів що зберігаються і обробляються пристроєм,

мінімізуючи ризики компрометації конфіденційної інформації підвищуючи захист і довіру до пристрою.

1.3.7. Insecure Data Transfer and Storage

Передача і зберігання даних у відкритому вигляді є серйозною проблемою для IoT. Причиною відсутності цих механізмів можуть бути слабкі обчислювальні потужності пристроїв або недобросовісність виробників IoT пристроїв. Більшість IoT збирають як чутливу інформацію так і особисті дані користувачів. Зловмисники можуть маніпулювати цими даними під час їх передачі або отримувати до них доступ якщо вони зберігаються в локальній базі даних. Наприклад, якщо пристрій використовує протокол передачі даних файлів FTP(File Transfer Protocol) для обміну даними, зловмисники можуть перехопити ці дані і, наприклад, замінити його, що призведе не тільки до витоку чутливої інформації, а й до порушення роботи системи. Використання небезпечного протоколу HTTP(Hyper Text Transer Protocol) для передачі даних через інтернет також може спричинити втрату конфіденційної або чутливої інформації. Для вирішення цієї проблеми, перше що спадає на думку, це використання безпечних протоколів для передачі даних, HTTP може замінити HTTPS(Hyper Text Transer Protocol Secure), це версія застарілого протоколу HTTP що використовує шифрування при передачі даних. Протокол для передачі даних FTP можна замінити його безпечною версією SFTP(Secure File Transfer Protocol), як і у випадку з HTTPS, цей протокол використовує механізми шифрування для передачі даних що і підвищує його безпеку. З використанням шифрування для передачі даних, не варто забувати про шифрування даних які зберігаються на пристрої, ці дані також повинні бути зашифровані щоб унеможливити їхнє викрадення. Запровадження механізмів контролю доступу, дозволить запобігти доступу зловмисника до даних які зберігаються на пристрої в першу чергу, це може стати одним з етапом захисту інформації. Ці заходи дозволять створити

надійну систему захисту даних під час передачі та зберігання, знижуючи ризики пов’язані з маніпуляцією і викраденням даних.

1.3.8. Absence of Device Management

Неефективне управління системою IoT пристроїв створює серйозну загрозу безпеки всієї мережі. Відсутність належного управління дозволяє зловмисникам маніпулювати або контролювати IoT пристрої. Недостатній рівень управління може призвести до несанкціонованого доступу, маніпуляцій з пристроями або модифікації прошивки. Наприклад застарілі SSL(Secure Socket Layer) сертифікати можуть призвести до переходу на небезпечний протокол HTTP для комунікацій, оскільки пристрій не отримує оновлення сертифікатів це робить його вразливим до атак. Вирішити цю проблему можуть впровадження надійних механізмів автентифікації і реалізація засобів контролю доступу. Завдяки тому що кожен користувач буде власний унікальний обліковий запис, можна застосувати розмежування доступу, zero-trust або інші підходи які позитивно впливають на безпеку системи.

1.3.9. Insecure Default Settings

При встановлені нового IoT пристрою, вони зазвичай вже мають певні початкові налаштування які обов’язково необхідно змінити. Зазвичай ці налаштування є небезпечними, оскільки розробники очікують від користувача зміни цих налаштувань з метою персоналізації під свої потреби, але дуже часто ці налаштування не змінюються, що підвищує вразливість пристрою до атак. Сюди входять конфігурації встановлені за замовчуванням, такі як типові імена користувачів, паролі, відкриті порти, незашифровані комунікації і тд. Зміна стандартних облікових даних та конфігурації пристрою під час початкового налаштування пристрою вирішить цю проблему. Це дозволить запобігти легкому доступу зловмисників через стандартні облікові дані. Також, щоб зменшити

площину для атак, необхідно позбутись непотрібних сервісів і портів. Цей крок не тільки збільшить безпеку пристрою, а й підвищить продуктивність зменшивши навантаження. Ці два кроки сприяють покращенню безпеки і продуктивності IoT пристроїв, знижуючи ризики їх компрометації через використання типових налаштувань.

1.3.10. Lack of Physical Hardening

Останньою але не менш важливою проблемою є відсутність фізичного захисту IoT пристроїв. Це може становити перешкоду для забезпечення безпеки, роблячи їх вразливими до атак на апаратну складову, таких як підміна прошивки. Результатом таких атак може бути несанкціонований доступ з привілеями root користувача. Завдяки цьому зловмисник може закріпитись на девайсі і використовувати його для віддалених атак або для управління ним. Для забезпечення безпеки фізичного доступу існує ряд кроків які дозволяють цього добитись. Відключення або ізоляція пристроїв та портів для дебагу – обмежує можливість прямого доступу до апаратного забезпечення. Використання перевірки цілісності прошивки дозволяє запобігти несанкціонованим модифікаціям. Впровадження механізмів виявлення спроб фізичного втручання – сигналізує про можливе втручання з боку зловмисників. Не зберігати чутливу або конфіденційну інформацію на змінних картах пам’яті – це мінімізує ризики їх викрадення у випадку несанкціонованого фізичного доступу.

РОЗДІЛ 2. ТЕОРЕТИЧНІ ОСНОВИ ТЕСТУВАННЯ БЕЗПЕКИ IOT

2.1. Співвідношення OWASP IoT TOP 10 і рекомендацій ENISA

Забезпечення безпеки IoT є одним з ключових викликів сучасної кібербезпеки. Вразливості IoT впливають не лише на конфіденційність і доступність даних, але й на фізичну безпеку користувачів, що робить їх потенційними цілями для кіберзлочинців. Для систематизації знань та вирішення цих проблем створюються міжнародні стандарти і рекомендації, серед яких OWASP IoT Top 10 та ENISA Baseline Security Recommendations є одними з найвідоміших. Кожен із цих документів має свої особливості: OWASP IoT Top 10 акцентує увагу на найпоширеніших технічних вразливостях IoT, а ENISA пропонує ширший підхід, інтегруючи технічні, організаційні та юридичні аспекти безпеки.

OWASP IoT Top 10 фокусується на практичних вразливостях, таких як слабкі паролі, відсутність шифрування або небезпечні налаштування за замовчуванням. ENISA ж охоплює додаткові аспекти, наприклад, управління життєвим циклом пристроїв, тренінги для співробітників, взаємодію з третіми сторонами та управління інцидентами. Це дозволяє ENISA формувати рекомендації не лише для розробників пристроїв, але й для організацій, які інтегрують IoT у свої бізнес-процеси.

2.1.1. Security by design

Рекомендації ENISA щодо безпеки IoT пристроїв підкреслюють важливість інтеграції безпеки на всіх етапах життєвого циклу системи — від проектування до впровадження. Зокрема, необхідно враховувати безпеку не тільки пристрою, але й всієї екосистеми IoT, інтегруючи політики безпеки, що дозволяють обробляти різні рівні загроз.

Важливим є також те, щоб безпека пристроїв не ставала на заваді іншим важливим факторам, таким як збереження енергії. Наприклад, іноді економія енергії може призводити до використання слабших алгоритмів шифрування, що підвищує ризик атак. Крім того, проектування архітектури IoT пристроїв має передбачати компартменталізацію для захисту системи від внутрішніх і зовнішніх атак, що є схожим на рекомендації OWASP IoT Top 10 щодо безпеки програмного забезпечення та обмеження доступу до критичних компонентів.

Щодо тестування, ENISA наголошує на важливості проведення тестів на проникнення, що допомагає виявити слабкі місця у обробці введених даних або автентифікації — це тісно пов'язано з рекомендаціями OWASP IoT Top 10, які зосереджуються на важливості належної обробки даних і захисту від несанкціонованого доступу. Також для розробників важливим є проведення рев'ю коду для запобігання вразливостям, що відповідає принципам безпеки OWASP, які зосереджені на виявленні та усуненні проблем ще на етапі розробки.

2.1.2. Privacy by design

Що стосується конфіденційності в системах IoT, ENISA наголошує на необхідності забезпечення конфіденційності на всіх етапах проектування системи. Зокрема важливо щоб захист конфіденційності був невід’ємною частиною самого дизайну пристрою, що означає що на кожному етапі розробки будуть визначені і реалізовані механізми для забезпечення конфіденційності. Іншою важливою рекомендацією є обов’язкове проведення privacy impact assessment перед запуском нових додатків. Такий тест дозволяє виявити потенційні ризики для конфіденційності перед релізом, і дає можливість або виправити недолік або підготуватись до ймовірних ризиків. Ці принципи безпосередньо пов’язані з OWASP IoT Top 10 – Lack of a Proper Privacy Protection. Відсутність належного захисту конфіденційності може призвести до витоку особистих даних, порушення приватності користувачів і порушення

законодавчих вимог. Отже, інтеграція конфіденційності в дизайн є необхідною для зниження ризиків пов’язаних з недостатнім захистом приватності.

2.1.3. Asset Management

Говорячи про управління активами, ENISA підкреслює важливість розробки та підтримки процедур управління активами та контролю конфігурацій для ключових систем. Це означає що потрібно мати чітко визначену стратегію для відстеження та управління всіма пристроями та компонентами в системі, а також забезпечити контроль над їх конфігурацією. Іншими словами – всі пристрої в системи мають бути ідентифіковані, класифіковані і промоніторені, а їх конфігурація чітко задокументована. Це дозволяє швидко реагувати на потенційні загрози або вразливості, а також забезпечує більш ефективне управління ресурсами. Ця рекомендація відноситься до OWASP IoT Top 10 – Absence of device management. Відсутність адміністрування може призвести до втрати контролю над пристроєм. Правильне управління активами є критичним для підтримання цілісності та безпеки всієї IoT системи, оскільки дозволяє вчасно захищати компоненти системи.

2.1.4. Strong Default Security and Privacy

У рекомендаціях ENISA щодо безпеки IoT пристроїв приділяється особлива увага питанню слабких, легких або hardcoded паролів, оскільки це є однією з основних вразливостей, що може поставити під загрозу цілісність системи. ENISA пропонує, щоб розробники апаратного забезпечення та програмного забезпечення для IoT впроваджували тестування на проникнення для перевірки наявності таких вразливостей. Це тестування допомагає виявити недоліки в обробці інпуту, спроби обхід автентифікації та інші проблеми, які можуть виникнути через неправильно налаштовані або зашиті паролі.

Якщо в пристрої або програмному забезпеченні використовуються прості або стандартні паролі, це значно підвищує ризик того, що зловмисник може вгадати пароль і отримати доступ до системи. Більш того, коли паролі закодовані прямо в коді, їх дуже легко витягнути, що робить систему вразливою до атак. Враховуючи ці ризики, важливо забезпечити, щоб усі паролі були складними, унікальними та не були закодовані в коді. Тому регулярне тестування на проникнення є ефективним способом для виявлення таких вразливостей.

Ця рекомендація ENISA відображає проблеми, описані в OWASP IoT Top 10, зокрема в категорії слабких паролів. Вона підкреслює важливість забезпечення належного рівня безпеки на етапі розробки та тестування пристроїв. Виявлення і усунення вразливих паролів на ранніх етапах може значно знизити ризики для системи. Одним із найбільш ефективних методів є застосування складних паролів, що містять випадкові комбінації символів, а також забезпечення можливості зміни пароля користувачем. Важливим аспектом є також відмова від практики жорстко закодованих паролів у програмному забезпеченні, що є одним із основних напрямів роботи для розробників, які прагнуть підвищити безпеку своїх пристроїв.

2.1.5. Secure and Trusted Communications

Одним із ключових викликів у сфері безпеки IoT пристроїв є ненадійні мережеві служби, які несуть серйозні ризики для користувачів та інфраструктури. Рекомендації ENISA з цього питання підкреслюють необхідність належного управління активами та конфігураціями. Особливу увагу слід приділяти встановленню й підтримці процедур, які забезпечують безпеку ключових мережевих і інформаційних систем. Ненадійні мережеві служби можуть включати відкриті порти, які не використовуються, або служби, що не мають належного рівня захисту, таких як шифрування трафіку чи автентифікація. Відсутність контролю над такими аспектами може призводити до експлуатації пристроїв зловмисниками для використання пристрою для атак

типу DDoS або використання пристроїв як точки входу для подальших вторгнень у мережу. ENISA рекомендує застосовувати принципи управління конфігурацією, щоб звести до мінімуму поверхню атаки. Це включає регулярний моніторинг мережевої активності пристроїв, перевірку відкритих портів та відключення непотрібних служб. Такі заходи можуть запобігти несанкціонованому доступу до пристроїв. Додатково, важливим аспектом є впровадження багаторівневих механізмів автентифікації, які значно ускладнюють доступ для зловмисників.

Ці рекомендації тісно пов’язані з пунктом Insecure Network Services з OWASP IoT Top 10. В обох документах підкреслюється, що слабкий контроль за мережевими службами створює значні ризики для безпеки. До прикладу, залишені відкритими порти або слабке шифрування дозволяють зловмисникам перехоплювати трафік, змінювати дані або виконувати атаки на пристрої. Управління мережевими службами є основою для захисту IoT пристроїв, оскільки саме через ненадійні мережеві служби зловмисники найчастіше знаходять способи компрометації. Завдяки регулярним перевіркам, впровадженню заходів контролю конфігурації та шифрування даних можна забезпечити високий рівень безпеки IoT екосистеми.

2.1.6. Secure Interfaces and Network Services

Проблема ненадійних інтерфейсів екосистеми є однією з ключових загроз безпеки IoT пристроїв. Ці інтерфейси, які можуть включати веб-панелі керування, API або мобільні додатки, часто є точками взаємодії між користувачами та пристроями, а також між пристроями та серверними системами. Dразливості на цьому рівні можуть створювати можливості для зловмисників отримати несанкціонований доступ до конфіденційних даних, виконувати неавторизовані дії або навіть захопити контроль над пристроєм. Рекомендації ENISA з цієї теми зосереджуються на розробці надійних механізмів ідентифікації, автентифікації та авторизації. Зокрема, ENISA рекомендує

розробникам програмного забезпечення проводити регулярні рев’ю коду, щоб виявляти та виправляти помилки ще на етапі розробки. Також акцентується увага на впровадженні чітких політик керування доступом, які обмежують права користувачів та програм до мінімально необхідного рівня.

Ця рекомендація перегукується з пунктом Insecure Ecosystem Interfaces з OWASP IoT Top 10, який описує загрози, пов'язані з неналежним захистом API, інтерфейсів управління та хмарних служб. Зокрема, слабкі механізми автентифікації або недостатня перевірка введених даних можуть призвести до експлуатації цих інтерфейсів для виконання шкідливих дій. Такі атаки можуть включати викрадення облікових даних, експлуатацію ін’єкційного коду або виконання дій від імені адміністратора системи. Щоб знизити ці ризики, ENISA рекомендує впроваджувати багатофакторну автентифікацію, використовувати стандартизовані протоколи захисту, такі як OAuth2, а також регулярно проводити тестування на проникнення для перевірки безпеки інтерфейсів. Важливо також забезпечити шифрування всіх даних, які передаються між пристроями та інтерфейсами, щоб запобігти їх перехопленню зловмисниками.

Таким чином, забезпечення надійності екосистемних інтерфейсів є критично важливим для захисту IoT пристроїв і даних користувачів. Це вимагає інтеграції безпеки в процес розробки, дотримання кращих практик з автентифікації та захисту даних, а також регулярного тестування для виявлення потенційних вразливостей.

2.1.7. Secure Software/ Firmware Updates

Відсутність надійного механізму оновлення є серйозною вразливістю для IoT пристроїв, яка може дозволити зловмисникам використовувати застаріле програмне забезпечення з відомими вразливостями. Ненадійний механізм оновлення може також бути використаний для розповсюдження шкідливого коду або для виконання атак типу "man-in-the-middle", де зловмисник змінює або перехоплює оновлення. Рекомендації ENISA наголошують на необхідності

розробки безпечних механізмів оновлення програмного забезпечення, які повинні включати перевірку автентичності оновлень перед їх встановленням. Виробникам рекомендується використовувати цифрові підписи для кожного оновлення, щоб гарантувати, що воно походить від довіреного джерела. Також важливим аспектом є застосування захищених каналів передачі для доставки оновлень, таких як протоколи HTTPS або TLS, що забезпечують шифрування трафіку і захищають дані від перехоплення.

Ця рекомендація тісно перегукується з пунктом Lack of Secure Update Mechanism з OWASP IoT Top 10, який акцентує увагу на ризиках, пов'язаних з відсутністю належного контролю за процесом оновлення. Наприклад, якщо оновлення встановлюється без перевірки його джерела, зловмисники можуть вставити шкідливий код, що призведе до компрометації пристрою або мережі. Окрім безпеки самого механізму оновлення, ENISA також рекомендує забезпечити можливість для користувачів легко перевіряти та встановлювати оновлення. Це включає в себе автоматичні оновлення, які працюють без втручання користувача, але при цьому надають йому інформацію про зміни, які впроваджуються. Запровадження безпечних механізмів оновлення є не лише питанням технічного виконання, а й організаційною вимогою. Компанії-виробники повинні гарантувати, що оновлення підтримуються протягом усього життєвого циклу пристрою. Це особливо важливо для критичних інфраструктур, де відсутність оновлення може мати катастрофічні наслідки. Зрештою, забезпечення надійного механізму оновлення — це ключовий крок для мінімізації ризиків і підтримання довіри користувачів до IoT пристроїв. Впровадження криптографічних методів перевірки автентичності, захищених каналів зв'язку та автоматизованого оновлення допомагає створити систему, яка здатна протистояти сучасним кіберзагрозам.

2.1.8. Proven Solutions

Використання небезпечних або застарілих компонентів є однією з найбільш поширених проблем у сфері безпеки IoT пристроїв. Такі компоненти, як застарілі бібліотеки, модулі або операційні системи, можуть містити відомі вразливості, які зловмисники легко використовують для компрометації пристрою або мережі. Особливу небезпеку становлять компоненти з публічно відомими вразливостями, для яких вже існують експлойти. ENISA пропонує застосовувати активний підхід до управління компонентами. Це включає створення та підтримку процедур управління активами, які дозволяють ідентифікувати всі використовувані компоненти, їх версії та статус підтримки. Крім того, ENISA наголошує на важливості використання тільки перевірених і підтримуваних компонентів, що мають актуальні оновлення безпеки. Регулярний аудит системи допомагає виявити застарілі або небезпечні компоненти, які необхідно оновити або замінити.

Ця рекомендація безпосередньо пов’язана з пунктом Using Insecure or Outdated Components з OWASP IoT Top 10. В обох випадках акцент робиться на тому, що небезпечні компоненти можуть стати основою для експлуатації всієї системи. Наприклад, використання застарілих криптографічних бібліотек або небезпечних протоколів, таких як FTP, робить пристрої вразливими до атак типу "man-in-the-middle" або до розшифрування даних зловмисниками. Одним із ключових підходів до вирішення цієї проблеми є впровадження системи моніторингу вразливостей, яка дозволяє автоматично отримувати сповіщення про нові вразливості, що стосуються використовуваних компонентів. Також важливо враховувати питання ліцензування компонентів, щоб уникнути використання тих, які більше не підтримуються розробниками. Крім того, важливим є регулярне проведення тестів на проникнення, які допомагають виявляти вразливості пов’язані з застарілими компонентами. Тестування дозволяє зрозуміти, як саме ці вразливості можуть бути використані зловмисниками, та розробити відповідні заходи з їх усунення.

2.1.9. Trust and Integrity Management

Небезпечні налаштування за замовчуванням є однією з головних загроз для безпеки IoT пристроїв. Часто виробники залишають стандартні паролі, відкриті порти або непотрібні служби активними, щоб полегшити налаштування та використання пристроїв. Проте такі налаштування створюють значні ризики, оскільки зловмисники можуть легко знайти ці "відомі" конфігурації та використати їх для атак. Рекомендації ENISA підкреслюють важливість забезпечення безпеки вже на етапі розробки пристроїв. Це включає обов'язкове впровадження безпечних налаштувань за замовчуванням, таких як вимкнення непотрібних служб і протоколів, закриття небезпечних портів і налаштування складних паролів, які користувач має змінити при першому використанні. Виробникам також слід забезпечити легкий доступ до інструкцій із налаштування пристрою, щоб користувачі могли швидко й правильно змінити конфігурацію.

Ця рекомендація безпосередньо перегукується з пунктом Insecure Default Settings з OWASP IoT Top 10. Обидва документи наголошують, що стандартні налаштування часто не враховують реальних загроз і є легкою мішенню для атак. Наприклад, стандартні облікові дані адміністратора, які часто залишаються незмінними, дозволяють зловмисникам отримати повний контроль над пристроєм. Щоб зменшити ці ризики, ENISA рекомендує використовувати підхід "захищено за замовчуванням" (secure by default). Це означає, що пристрій повинен бути максимально захищеним одразу після активації, а будь-які додаткові функції мають увімкнутися лише за рішенням користувача. Наприклад, замість активного за замовчуванням віддаленого доступу, він має бути вимкненим, якщо в цьому немає гострої необхідності. Крім того, тестування на проникнення та аудит конфігурацій повинні бути інтегровані в процес розробки та підтримки пристроїв. Це дозволяє виявляти небезпечні налаштування до того, як пристрій потрапить у руки користувача. Важливим є і

навчання кінцевих користувачів щодо важливості зміни стандартних налаштувань і базових принципів безпеки.

2.1.10. Hardware Security

Відсутність фізичного захисту є серйозною вразливістю в IoT пристроях, яка дозволяє зловмисникам отримати доступ до апаратного забезпечення для виконання шкідливих дій. Це може включати розкриття корпусу пристрою для прямого доступу до компонентів, маніпуляцію з портами для перехоплення даних або навіть перепрограмування мікроконтролерів для зміни поведінки пристрою. Рекомендації ENISA наголошують на важливості інтеграції фізичних заходів захисту в дизайн пристроїв. Серед ключових заходів — використання герметичних корпусів, які захищають внутрішні компоненти від доступу без інструментів або помітного пошкодження. Також пропонується впровадження засобів захисту від несанкціонованого втручання, таких як пломби або спеціальні сенсори, що можуть виявляти відкриття корпусу і блокувати функціонування пристрою в разі порушення.

Ця проблема тісно пов'язана з пунктом Lack of Physical Hardening із OWASP IoT Top 10. Він підкреслює, що фізичний доступ до пристрою може дозволити зловмиснику виконати низку атак, включаючи перехоплення комунікацій, підключення до внутрішніх шин даних, таких як I2C або SPI, або навіть вилучення ключів шифрування, які зберігаються в пристрої. Одним із ефективних способів зменшити ризики є впровадження апаратних засобів безпеки, таких як апаратні модулі довірчої платформи (TPM) або захищені елементи (Secure Elements), які забезпечують ізоляцію конфіденційних даних навіть у разі фізичного доступу до пристрою. Крім того, ENISA рекомендує мінімізувати доступні фізичні інтерфейси, такі як USB або UART, якщо вони не є критично необхідними для роботи пристрою. Також важливим є забезпечення захисту прошивки та завантажувального процесу. Наприклад, використання цифрових підписів для верифікації програмного забезпечення дозволяє

гарантувати, що навіть при фізичному доступі зловмисник не зможе змінити прошивку без виявлення.

2.2. Інструменти для ідентифікації вразливостей у IoT-пристроях

2.2.1. Reconnaissance

Перший етап cyber kill chain — «розвідка». На цьому етапі зловмисник збирає інформацію про ціль, наприклад, визначає потенційні вразливості, ключовий персонал, конфігурацію мережі та встановлює заходи безпеки використовуються. Ця фаза може включати пасивні методи, такі як збір розвідувальних даних з відкритих джерел (OSINT) або активне сканування системи цілі. Розвідка може відбуватися як онлайн, так і офлайн, при цьому зловмисники використовують різні методи, щоб отримати уявлення про слабкі місця своєї цілі. Цей етап також включає тестування на проникнення для визначення потенційних точок входу, допомагаючи зловмисникам планувати свої наступні дії. Розуміння першого етапу cyber kill chain допомагає спеціалістам з безпеки з Blue Team передбачати та пом’якшувати загрози до їх ескалації.

Nmap (Network Mapper) це основа основ всіх тестувань на проникнення, зокрема на стадії розвідки. Цей інструмент спроектовано для сканування мереж, через це, він став незамінним інструментом для спеціалістів з кібербезпеки для збору інформації про мережу, зокрема які девайси є в мережі та інформацію безпосередньо про самі пристрої. Nmap відомий за свою функціональність і точність. Він надає ряд важливої інформації про пристрої в мережі, зокрема:

- IP-адреси: Nmap ідентифікує адреси пристроїв і класифікує їх за тим які протоколи вони використовують.
- відкриті порти: Визначає відкриті порти що можуть стати потенційними точками входу. Наприклад, IoT пристрої зазвичай мають веб-інтерфейс на 80 або 443 порті.

- визначення операційної системи та даних про прошивку: з допомогою Nmap, пентестер може визначити операційну систему цілі та версію прошивки, що дасть можливість ідентифікувати застарілі версії системи з відомими вразливостями.
- визначення сервісів: Nmap скануючи порти, виявляє також які сервіси працюють на цих портах. Наприклад на 21 порт використовується сервісом FTP, 22 – SSH, 80 – http. Всі ці сервіси можуть бути застарілими або неправильно сконфігурованими, чим і може скористатись зловмисник.

2.2.2. Weaponization

Етап озброєння cyber kill chain відбувається після того, як проведена розвідка, і зловмисник зібрав достатньо інформації про потенційні цілі та їхні вразливі місця. Під час цього етапу зловмисник створює або отримує зловмисне корисне навантаження, наприклад шкідливе програмне забезпечення або шкідливий документ, який призначений для використання конкретних вразливостей, виявлених на етапі розвідки.

Weaponization може передбачати розробку нових типів зловмисного програмного забезпечення або модифікацію існуючих інструментів для використання в атаці. Наприклад, кіберзлочинці можуть внести незначні зміни в існуючий варіант програми-вимагача, щоб створити новий інструмент. Ця фаза також включає підготовку корисного навантаження для досягнення цілей зловмисника, водночас потенційно впроваджуючи заходи для уникнення виявлення рішеннями безпеки. Розуміння використання зброї допомагає захисникам передбачити, як зловмисники можуть створювати свої інструменти.

Приклади цього етапу cyber kill chain в реальному світі включають налаштування зловмисного програмного забезпечення для обходу антивірусного програмного забезпечення або створення фішингових електронних листів із вкладеннями для використання необізнаності або необережності користувачів.

Існує декілька потужних інструментів які можна використовувати на цій стадії, один з таких RouterSploit.

RouterSploit є спеціалізованим інструментом для тестування безпеки мережевих пристроїв, зокрема IoT. Його розроблено з акцентом на експлуатацію вразливостей у таких пристроях, як маршрутизатори, камери спостереження, точки доступу Wi-Fi та інші IoT-системи. На етапі Weaponization у Cyber Kill Chain RouterSploit дозволяє підготувати експлойти для атак, базуючись на виявлених під час розвідки вразливостях. Цей інструмент пропонує набір модулів, подібних до Metasploit, але з більш вузькою спеціалізацією, орієнтованою саме на IoT та мережеві пристрої.

Під час Weaponization, RouterSploit дозволяє ідентифікувати відомі вразливості, які можна експлуатувати, та забезпечує засоби для їхньої реалізації. Зокрема, він підтримує автоматизовані атаки, такі як брутфорс облікових даних або використання некоректно налаштованих API. Інструмент має модулі для тестування конкретних протоколів, таких як Telnet чи SSH, які часто використовуються в IoT-пристроях. Це дозволяє перевіряти, чи може слабка автентифікація або незахищене передавання даних бути використане зловмисниками.

Наприклад, якщо IoT-пристрій має відкритий Telnet-порт і використовує стандартні облікові дані, RouterSploit може бути використаний для проведення автоматизованого брутфорсу. Встановивши з'єднання з пристроєм, інструмент дозволяє тестувальнику налаштувати подальші дії, такі як отримання доступу до конфігураційного файлу або аналіз мережевих налаштувань.

RouterSploit також забезпечує простий інтерфейс для створення власних модулів експлойтів, що робить його зручним для моделювання спеціалізованих атак. Завдяки цьому він є ефективним інструментом для тестування безпеки IoT у реальних умовах, дозволяючи тестувальникам налаштовувати сценарії атак і перевіряти, наскільки вони можуть бути успішними в різних середовищах.

2.2.3. Delivery

Етап «Delivery» з Cyber Kill Chain — це етап, на якому зловмисник передає зловмисне корисне навантаження на цільову систему. Це може статися різними способами, зокрема фішинговими електронними листами, інфікованими вкладеннями або шкідливими веб-сайтами. Delivery має вирішальне значення для прогресу атаки, оскільки вона закладає основу для виконання зловмисного корисного навантаження.

Окрім традиційних методів, доставка також може передбачати злом мереж і використання вразливостей програмного чи апаратного забезпечення. Зловмисники можуть використовувати методи соціальної інженерії, щоб збільшити ймовірність успіху. Знання того, як зловмисник здійснить кібератаку, допомагає захисникам застосовувати такі заходи, як виявлення зловмисного програмного забезпечення та вбудоване сканування загроз, щоб перехопити ці корисні навантаження, перш ніж вони досягнуть цілей. Ефективні приклади Delivery Cyber Kill Chain включають надсилання фішингових електронних листів із шкідливими вкладеннями або використання відомої вразливості в мережевому програмному забезпеченні для отримання несанкціонованого доступу та доставки зловмисного програмного забезпечення. Вибір інструментів на цьому етапі дуже залежить від того скільки і яка інформація була зібрана на першому етапі розвідки. Якщо ціль має вразливий сервер електронної пошти, можна скористатись Nmap. Окрім розвідки, цей інструмент дає великий вибір експлойтів які можуть бути використані зокрема для атак на сервери електронної пошти. Якщо компанія не турбується про безпеку емейлів, можна скористатись фішингом.

2.2.4. Exploitation

Етап «Exploitation» Cyber Kill Chain представляє критичний момент, коли зловмисники активно користуються виявленими вразливими місцями для

виконання своїх експлойтів. Цей етап є ключовим, оскільки він перетворює розвідувальні дані в активне вторгнення. Зловмисники використовують недоліки програмного забезпечення, неправильну конфігурацію або навіть недоліки соціальної інженерії, такі як фішингові атаки або скомпрометовані облікові дані, щоб зламати цільову систему. Цей процес може передбачати запуск експлойтів проти вразливого програмного забезпечення, використання слабких протоколів шифрування або використання параметрів за замовчуванням на пристроях IoT.

Успішне експлуатування відкриває двері для подальших зловмисних дій. Зловмисники можуть отримати несанкціонований доступ, підвищити привілеї та встановити контроль над системою. Наприклад, у середовищах IoT зловмисник може використати незахищений API або мережевий протокол із слабкою автентифікацією для доступу до конфіденційних функцій пристрою чи даних. Ці дії часто залишаються непоміченими в мережах, у яких відсутні ефективний моніторинг або сегментація, що дозволяє зловмисникам залишатись непоміченими.

Після виконання корисного навантаження зловмисники можуть використовувати методи бічного переміщення (Lateral movement), щоб досліджувати та скомпрометувати додаткові системи в мережі. Це може включати встановлення шкідливих інструментів, розгортання скриптів для збору конфіденційних даних або зміну конфігурацій безпеки, наприклад вимкнення брандмауерів або антивірусного захисту. Ці дії не тільки зміцнюють опору зловмисника, але й служать підготовчими кроками до останніх етапів атаки, таких як викрадання даних або саботаж системи.

Відсутність механізмів обману, таких як приманки (Honeypot), додатково полегшує навігацію зловмисника. Без цих заходів мережа не зможе вводити в оману або сповільнювати зловмисників, надаючи їм більшу свободу пересування. Етап експлуатації підкреслює важливість проактивних заходів безпеки, включаючи регулярне сканування вразливостей, своєчасне керування виправленнями та впровадження систем виявлення та реагування на хостах (EDR).

Для тих, хто захищає систему, розуміння стадії експлуатації забезпечує структуру для переривання ланцюжка атак. Зосереджуючись на ймовірних векторах використання, таких як вразливі системи, неправильно налаштовані пристрої або слабкі облікові дані, команди безпеки можуть сильно посилити захист системи. Такі методи, як системи виявлення вторгнень (IDS), регулярне тестування на проникнення та застосування принципів найменших привілеїв, можуть значно знизити ймовірність успіху експлуатації. Крім того, інструменти моніторингу, які виявляють аномальну поведінку під час експлуатації, можуть забезпечити швидший час реакції, мінімізуючи потенційну шкоду.

Цей етап підкреслює динамічну природу кіберзахисту, де передбачення та адаптація є ключовими для випередження досвідчених супротивників. Аналізуючи методи використання та розробляючи надійні заходи безпеки, організації можуть ефективно запобігати атакам до того, як вони перейдуть до наступного етапу Cyber Kill Chain.

Говорячи про цей етап, не можна не згадати Burp Suite. Burp Suite це інструмент для тестуваннь на проникнення розроблений компанією PortSwigger. Він надає повний набір інструментів для виявлення та використання вразливостей у веб-додатках, API та навіть пристроях IoT, які покладаються на веб-інтерфейси. Під час експлуатації зловмисники використовують Burp Suite для виконання зловмисних корисних навантажень, перевірки слабких конфігурацій і використання виявлених вразливостей для отримання несанкціонованого доступу або підвищення привілеїв. Burp Suite має багато модулів які активно використовуються для атак, найпопулярніші з них включають:

- Intruder. Цей модуль дозволяє створювати корисні навантаження для багатьох атак і проводити автоматизовані атаки, як от брутфорс.
- Repeater. Дозволяє багаторазово відправляти відредаговані http-запити, що значно покращує досвід тестування веб-інтерфейсів.
- Proxy. Цей модуль призначений для перехоплення запитів з можливістю їхнього редагування для подальшої відправки.

Таким чином, Burp Suite є одним з найкращих інструментів для експлуатування вразливостей на стадії Exploitation. Можливість атакувати веб-інтерфейси IoT пристроїв підкреслює важливість цього інструменту в тестуванні на проникнення.

2.2.5. Installation

Після успішно проведеної атаки, отримавши доступ до цільової системи маючи навіть найнижчі привілеї, зловмисник переходить до фази «Інсталяції». На цьому етапі зловмисник намагається встановити зловмисне програмне забезпечення.

Цей етап передбачає налаштування інструментів, які дозволяють зловмиснику взяти під контроль систему та отримати дані які його цікавлять. Зловмисники можуть використовувати інтерфейси командного рядка, бекдори та трояни, щоб закріпитися в мережі. Створення бекдорів гарантує, що зловмисник зможе зберегти доступ до системи, навіть якщо вразливу точку в системі виявлено та закрито.

Ефективне встановлення дозволяє зловмисникам проникати в цільову мережу та виходити з неї непоміченими, полегшуючи подальшу експлуатацію та викрадання даних. Розуміння цього етапу Cyber Kill Chain має вирішальне значення для захисників, щоб реалізувати заходи, які виявляють і запобігають шкідливим установкам, таким чином захищаючи цілісність мережі.

Таке програмне забезпечення називають «Руткітами». Перший руткіт для Windows був написаний у 1999 році і назвали його NT Rootkit, сьогодні одним з найпопулярніших рукітів є «ZeroAccess rootkit». ZeroAccess використовується для завантаження інших зловмисних програм на уражені хости за допомогою ботнету, який раніше був пов’язаний з майнінгом біткоїну і «клік фраудами». Як і інші сучасні руткіти, він розроблений таким чином, щоб залишатися непоміченим у цільових системах.

Після початкового зараження ZeroAccess перезаписує основні системні файли Windows і встановлює перехоплювачі ядра, намагаючись залишатися прихованим. Після встановлення хуків операційна система переходить під контроль руткіту, який потім може приховувати процеси, файли та мережеву активність, а також вбивати будь-яке антивірусне програмне забезпечення, яке намагається отримати доступ до процесів або файлів трояну.

Може здатись, що основною метою шкідливого програмного забезпечення є отримання доходу за допомогою реклами з оплатою за клік, так званий «клік фрауд». Проте, ZeroAccess, встановлює бекдор, щоб дозволити підключення до C2 сервера. Це, в свою чергу, надає віддаленому зловмиснику повний доступ до скомпрометованої системи.

2.2.6. Command and Control

«Command and Control» (C2) — це етап, на якому зловмисник встановлює зв’язок із скомпрометованою системою чи мережею. Цей зв’язок дозволяє зловмиснику зберігати контроль, передавати команди та отримувати дані від скомпрометованих систем. Це критичний етап, оскільки він забезпечує постійну взаємодію та контроль над ціллю.

Під час фази C2 зловмисники використовують успішно встановлене зловмисне програмне забезпечення для дистанційного керування пристроями чи ідентифікаторами в мережі цілі. Вони також можуть поширюватись на інші хости, щоб уникнути виявлення та встановити додаткові точки входу. Прикладом такого зв’язку є випадки, коли зловмисники використовують сервери C2, щоб наказувати комп’ютерам які, заражені зловмисним програмним забезпеченням, таким як ботнет Mirai, перевантажувати веб-сайт трафіком, спричиняючи атаку розподіленої відмови в обслуговуванні (DDoS). Іншим прикладом є надання вказівок скомпрометованим системам для виконання будь яких інших цілей, таких як викрадання даних або подальше проникнення в мережу.

2.2.7. Actions on Objectives

Етап «Actions on Objectives» є останнім кроком у Cyber Kill Chain, що представляє кінцеву мету зловмисника. Цей етап настає після того, як кіберзлочинці розробили своє шкідливе ПЗ, встановили його в мережу цілі та взяли під контроль системи. Цілі зловмисника можуть бути різними та включати крадіжку даних, саботаж роботи системи, шифрування або викрадання даних.

Наприклад, зловмисники можуть викрасти конфіденційну інформацію, використовувати програмне забезпечення-вимагач як інструмент для вимагання або використати бот-мережу для запуску атаки розподіленої відмови в обслуговуванні (DDoS). Ця фаза означає завершення основної мети атаки, чи то зрив операцій, вилучення цінних даних або монетизація атаки через вимагання викупу.

2.3. Ідентифікація пристроїв у мережі.

Ідентифікація і документування всіх пристроїв в мережі є першим і одним з найважливіших етапів тестування безпеки. Метою цього процесу є визначення всіх підключених пристроїв, їх характеристик та особливостей взаємодії. Ця інформація дозволяє спеціалісту з кібербезпеки ефективно спланувати процес тестування та чітко визначити Scope. Ідентифікація пристроїв це сканування мережі з метою виявлення всіх підключених IoT пристроїв, до цього списку відносяться смарт-телевізори, колонки, камери відеоспостереження та інше. Для кожного з цих пристроїв має бути зібрана інформація про їх технічні характеристики. До цих характеристик входять назва і модель, інформація про прошивку, IP та MAC адреси, відкриті порти і служби які їх використовують. Таблиця 2.1 містить результати інвентаризації пристроїв домашньої мережі, яка була проведена перед початком тестування

Таблиця 2.1 – Інформація про пристрої у мережі

Номер	Назва	Модель	IP-адреса	MAC-адреса
1	LGWebOSTV	LG	192.168.0.183	1C:2F:A2:12:14:C4
2	NOMI-IPC	F42	192.168.0.197	08:ED:ED:23:F4:98
3	Mijia-vaccum	v2_mibt6857	192.168.0.199	58:B6:23:6B:68:57
4	IP-camera	Xiaomi	192.168.0.195	6C:22:1A:B3:90:4E
5	Smart-TV	Sony	192.168.0.200	90:B6:86:3D:01:9D
6	MITV	Xiaomi	192.168.0.192	00:12:43:A5:2D:0E

2.4. Методологія тестування мережі

У процесі оцінки захищеності мереж та пристроїв одним із ключових етапів є вибір і застосування чіткої методології тестування. Методологія — це систематизований підхід, що визначає порядок дій, інструменти та техніки, необхідні для досягнення конкретної мети тестування. Використання структурованої методології дозволяє забезпечити всебічний аналіз безпеки, уникнути пропусків у перевірці та забезпечити відтворюваність результатів.

На сьогодні існує багато загальновизнаних методологій тестування безпеки, таких як PTES (Penetration Testing Execution Standard), OSSTMM (Open Source Security Testing Methodology Manual), NIST SP 800-115, OWASP Testing Guide та MITRE ATT&CK. Кожна з цих методологій пропонує різні підходи для аналізу мереж, систем і пристроїв залежно від цілей тестування, рівня загроз та доступних ресурсів.

Однак специфіка IoT-пристроїв вимагає особливого підходу до тестування. На відміну від традиційних комп'ютерних систем, IoT-пристрої часто мають обмежені обчислювальні ресурси, нестандартні протоколи зв'язку та спрощені механізми захисту. Тому виникає необхідність у розробці власної методології, яка враховує особливості IoT-пристроїв у домашній мережі.

Метою розробки цієї методології є системна оцінка безпеки IoT-пристроїв у домашній мережі для виявлення вразливостей, що можуть бути використані зловмисниками. Розроблена методологія враховує специфіку IoT-пристроїв, а також потенційні ризики, пов’язані з їх підключенням до локальної мережі. Методологія складається з 5 основних етапів:

- інвентаризація пристроїв та збір інформації
- аналіз поверхні атаки та виявлення вразливостей
- перевірка конфігурацій безпеки
- експлуатація вразливостей
- документування та рекомендації

Етап інвентаризації пристроїв і збір інформації має на меті Ідентифікувати всі IoT-пристрої в домашній мережі та зібрати початкові дані для подальшого аналізу. На цьому етапі буде використано інструмент Nmap для сканування мережі і виявлення всіх пристроїв. Цим же інструментом буде зібрано інформацію про mac-адреси, порти, сервіси і операційну систему. За результатами сканування буде створено таблицю інвентаризації.

На наступному етапі, аналіз поверхні атаки та виявлення вразливостей, буде визначено потенційні вразливі точки у мережевій архітектурі та на пристроях. Для досягнення мети цього етапу буде проведено сканування відкритих портів та сервісів для виявлення зайвих або потенційно небезпечних служб, застарілих версій прошивки та відомих вразливостей які знаходяться у CVE базі та аналіз механізмів автентифікації.

На третьому етапі, перевірки конфігурацій безпеки, буде оцінюватись правильність налаштувань безпеки IoT-пристроїв. Зокрема буде перевірено наявність стандартних паролів, протоколів шифрування та аналіз логів для виявлення підозрілої активності.

Передостанній етап включає в себе експлуатацію вразливостей з метою оцінки можливих сценаріїв атак на основі виявлених вразливостей без завдання шкоди пристроям. Цей етап дозволить оцінити ризики від компрометації тих чи інших пристроїв і розробити сценарії реагування на інциденти.

Останній, але не менш важливий, етап передбачай документування знайдених проблем з безпекою і розробка рекомендації по їх усуненню або пом’якшенню наслідків від успішного експлуатування вразливостей зловмисниками.

Розроблена методологія забезпечує систематичний підхід до оцінки захищеності IoT-пристроїв у домашній мережі. Вона дозволяє ідентифікувати основні вразливості, проаналізувати потенційні загрози та запропонувати ефективні заходи для покращення безпеки.

РОЗДІЛ 3. ТЕСТУВАННЯ НА ПРОНИКНЕННЯ IOT ПРИСТРОЇВ У ДОМАШНІЙ МЕРЕЖІ

У сучасних умовах швидкого розвитку технологій Інтернету речей (IoT), безпека пристроїв, підключених до домашніх мереж, стає важливою складовою захисту інформації та приватності користувачів. IoT-пристрої, такі як смарт-камери, телевізори, побутова техніка та інші, зручні для використання, але часто мають вразливі конфігурації, недостатньо захищені мережеві протоколи або дефолтні налаштування, що відкривають можливості для атак зловмисників.

Практична частина цієї роботи присвячена аналізу захищеності IoT-пристроїв у домашній мережі з використанням авторської методології тестування. Метою тестування є виявлення вразливостей на різних рівнях – від конфігураційних налаштувань до фізичних загроз, а також пропозиція рекомендацій щодо покращення безпеки.

В основі тестування лежить системний підхід, що включає кілька етапів. Спочатку здійснюється інвентаризація всіх IoT-пристроїв у мережі та збір базової інформації про них. Далі виконується аналіз мережевих з'єднань і сервісів для виявлення можливих уразливих точок. На основі знайдених вразливостей проводиться теоретична симуляція атак, що дозволяє оцінити потенційні загрози без пошкодження пристроїв або даних. Завершальний етап включає документування результатів тестування та розробку рекомендацій щодо покращення захисту.

У цій частині дипломної роботи будуть детально описані етапи тестування, методи використаних інструментів і отримані результати. Це дозволить не лише оцінити поточний рівень безпеки IoT-пристроїв у домашній мережі, а й запропонувати практичні кроки для підвищення їх захищеності.

Дослідження проводилося в умовах домашньої мережі, що включає кілька IoT-пристроїв, таких як смарт-камери, телевізори, розумний пилосос та інші пристрої, підключені до локальної мережі через маршрутизатор. Використання домашньої мережі як середовища для сканування дозволяє виявити реальні

загрози та вразливості, характерні для побутових IoT-пристроїв. Структура мережі була такою: центральний маршрутизатор забезпечував підключення всіх пристроїв, частина з яких мала статичні IP-адреси, а інші — динамічні. Це дозволило провести повноцінне тестування за допомогою інструментів Nmap та інших сканерів.

3.1. Інвентаризація пристроїв та збір інформації

Інвентаризація пристроїв є першим і важливим етапом у процесі тестування безпеки IoT-пристроїв у домашній мережі. Вона полягає в ідентифікації всіх підключених до мережі пристроїв, визначенні їхніх основних характеристик та зборі інформації, що допоможе на подальших етапах тестування для виявлення вразливостей та потенційних загроз. Цей етап є основою для побудови загальної картини мережі та визначення рівня її захищеності.

Завданням інвентаризації є:

- виявлення всіх активних пристроїв, підключених до домашньої мережі.
- ідентифікація характеристик кожного пристрою, таких як IP-адреси, MAC-адреси, відкриті порти та сервіси, що працюють на пристроях.
- збір даних про прошивки, операційні системи та конфігурації пристроїв для подальшого аналізу на предмет вразливостей.

Для збору цієї інформації використовуються різноманітні інструменти та методи, один із найпоширеніших – це використання Nmap. Це потужний інструмент для сканування мережі, який дозволяє виявляти активні пристрої, визначати відкриті порти, ідентифікувати запущені сервіси та визначати операційні системи пристроїв. На таблиці буде представлено таблицю з усіма даними які вдалось зібрати з допомогою Nmap.

Таблиця 3.1 – Результат збирання даних про пристрої у мережі з допомогою Nmap

№	тип	IP	MAC	Відкриті порти	Операційна система
1	телевізор	192.168.0.183	1C:2F:A2:12:14:C4	1206, 1218, 1538, 1555, 1664, 1702, 3000, 3001, 18181, 36866	Linux 5.0 - 5.5
2	Айпі-камера	192.168.0.197	90:6A:94:86:D1:0B	80, 554, 8086	
3	Робот-пилосос	192.168.0.199	58:B6:23:6B:68:57	-	2N Helios IP VoIP doorbell (96%)
5	-	192.168.0.195		80, 554, 8899, 23000, 34567	Linux 3.2 - 3.16
6	-	192.168.0.198	90:B6:86:3D:01:9D	5555	-
7	телефон	192.168.0.199	F0:3D:03:C2:D6:E8		android

Для того щоб точніше визначити всі хости в мережі, було проведено додаткове сканування з допомогою ще одного сканера – Angry IP Scanner, схожого до Nmap. Angry IP Scanner – це швидкий і зручний інструмент для сканування хостів у мережі. Він дозволяє визначати активні хости та відкриті порти. До переваг можна віднести наявність графічного інтерфейсу, легке і швидке налаштування сканів, висока швидкість сканування завдяки багатопоточності і кросплатформеність. В порівнянні з Nmap, цей сканер має і деякі недоліки, а саме набагато менше можливостей налаштування для більш глибоко аналізу хостів і дуже обмежена підтримка скриптів і технік для сканування хостів. Незважаючи на недоліки, цей сканер дуже добре підходить для інвентаризації хостів у мережі. На таблиці 3.2 представлені результати сканування з допомогою цього сканера.

Таблиця 3.2. – Результати сканування мережі з допомогою Angry IP Scanner

№	IP	Hostname	Ports	MAC	Vendor
1	192.168.0.1	-	80,443	50:0F:F5:37:7E:10	TendaCo
2	192.168.0.185	-	-	28:D0:43:52:0A:32	-
3	192.168.0.200	Android.local	-	90:B6:86:3D:01:9D	Murata
4	192.168.0.193	Android-3.local	-	EC:FA:5C:FB:49:E5	Beijing Xiaomi
5	192.168.0.194	Android-2.local	-	46:DB:5F:E6:53:EF	-
6	192.168.0.195		80	6C:22:1A:B3:90:4E	-
7	192.168.0.197		80	90:6A:94:86:D1:0B	hangzhou
8	192.168.0.192	Android-4.local	-	82:51:71:5E:7F:E0	-
9	192.168.0.190	-	-	76:F6:E5:C7:C7:4C	-
10	192.168.0.196	-	-	42:86:F9:E7:E0:02	-
11	192.168.0.183	-	--	1C:2F:A2:12:14:C4	-
12	192.168.0.188	-		C0:35:32:70:DA:6B	-

3.2. Короткий аналіз результатів інвентаризації

Перший пристрій який буде проаналізовано це телевізор, який має IP-адресу 192.168.0.183 і MAC-адресу 1C:2F:A2:12:14:C4. Він працює на операційній системі Linux версії 5.0 - 5.5. На цьому пристрої відкрито кілька портів, зокрема 1206, 1218, 1538, 1555, 1664, 1702, 3000, 3001, 18181 та 36866. Ці порти можуть бути пов'язані з різними сервісами, такими як медіа-потоки, налаштування через веб-інтерфейси або адміністрування пристрою. Зокрема, порти 3000 і 3001, ймовірно, використовуються для доступу до веб-інтерфейсу телевізора, що може бути вразливим до атак, якщо цей інтерфейс не захищений паролем або якщо використовуються дефолтні паролі. Порт 18181, який може бути пов'язаний з мультимедійними сервісами, також відкритий, що може надавати можливість несанкціонованого доступу

Далі, IP-камера з IP-адресою 192.168.0.197 і MAC-адресою 90:6A:94:86:D1:0B працює на операційній системі, яка не визначена, але має відкриті порти 80 (HTTP), 554 (RTSP) та 8086. Порти 80 і 554 використовуються для медіа-стрімінгу та доступу до веб-інтерфейсу для налаштувань камери або

адміністрування. Порт 8086, ймовірно, також використовується для адміністрування пристрою. Враховуючи, що камери часто мають обмежену безпеку, існує ризик того, що вони можуть бути уразливими до атак через ці порти, особливо якщо веб-інтерфейс має слабкий пароль або не використовує шифрування для захисту даних. Порти для доступу до відео можуть також бути вразливими, якщо налаштування не обмежують доступ за IP-адресами або якщо використовуються дефолтні налаштування.

Робот-пилосос з IP-адресою 192.168.0.200 та MAC-адресою 58:B6:23:6B:68:57 не має відкритих портів за результатами сканування, але на основі MAC-адреси було встановлено, що пристрій є схожим на VoIP-дверний дзвінок 2N Helios. Це свідчить, що пристрій може використовувати операційну систему або прошивку, яка базується на Linux, і, ймовірно, має вразливості, характерні для подібних пристроїв. Оскільки не було виявлено відкритих портів, пристрій може бути налаштований на роботу в закритій мережі або обмежений у функціональності, що знижує ймовірність віддалених атак. Проте, на основі схожості з іншими пристроями, можна припустити, що пилосос може мати вразливості, пов'язані з використанням протоколів VoIP або іншими мережевими комунікаціями.

Пристрій з IP-адресою 192.168.0.195 не має ідентифікації, але працює на операційній системі Linux версії 3.2 - 3.16. Відкриті порти 80 (HTTP), 554 (RTSP), 8899, 23000 та 34567 можуть вказувати на різноманітні сервіси, такі як медіа-стрімінг або віддалене управління пристроєм. Порти 8899, 23000 та 34567 можуть бути пов'язані з менш стандартними протоколами, що використовуються для специфічних сервісів. Це може свідчити про наявність вразливостей, якщо ці порти не захищені належним чином, оскільки вони можуть бути потенційно доступні для атак через інтернет, якщо не налаштовані відповідні фільтри або правила доступу.

Пристрій з IP-адресою 192.168.0.198 і MAC-адресою 90:B6:86:3D:01:9D має відкритий лише один порт — 5555. Цей порт часто асоціюється з Android Debug Bridge (ADB), який дозволяє віддалений доступ до пристрою для налагодження.

Це є суттєвим ризиком безпеки, оскільки порт 5555 часто використовується зловмисниками для несанкціонованого доступу до Android-пристроїв. Якщо цей порт не закритий або пристрій не захищений належним чином, зловмисники можуть отримати доступ до пристрою, що створює загрозу для конфіденційності та цілісності даних.

Телефон з IP-адресою 192.168.0.199 і MAC-адресою F0:3D:03:C2:D6:E8 не є пристроєм IoT, тому його аналіз не потрібен.

Для точнішого аналізу IoT-пристроїв у домашній мережі було проведено сканування з використанням двох різних інструментів: Nmap та Angry IP Scanner**.** Ці два сканери є мають свої переваги і недоліки, оскільки мають різні підходи до процесу сканування, що забезпечує різний рівень глибини аналізу.

Ідентифікація пристроїв у результатах обох сканерів демонструє схожі показники. Зокрема, обидва інструменти виявили ті самі IP-адреси та MAC-адреси для кожного активного пристрою у мережі. Наприклад, IP-адреси 192.168.0.200 та 192.168.0.193 були успішно визначені обома сканерами з відповідними MAC-адресами, що свідчить про узгодженість результатів. Це підтверджує надійність виявлення пристроїв у межах мережі та зменшує ймовірність помилок у процесі сканування.

Важливо зазначити, що Nmap надає більше деталей щодо пристроїв завдяки можливості ідентифікації відкритих портів, операційних систем та версій сервісів. Це дозволяє використовувати Nmap для глибшого аналізу конфігурації та потенційних вразливостей IoT-пристроїв.

Angry IP Scanner відзначається вищою швидкістю сканування, що є перевагою для швидкого виявлення активних пристроїв у мережі. Цей інструмент зручний для початкового етапу дослідження, коли необхідно швидко зібрати базову інформацію про пристрої та їх відповіді на ping-запити. Проте через обмежену функціональність Angry IP Scanner не дозволяє проводити поглиблене тестування на проникнення чи визначати версії сервісів, що працюють на пристроях.

Ще однією важливою відмінністю є можливість розширеної конфігурації Nmap, яка включає різні режими сканування, наприклад сервісне сканування (-sV) та визначення операційної системи (-O). Ці режими можуть допомогти ідентифікувати навіть ті пристрої, які не відповідають на стандартні запити, що робить Nmap ефективнішим для виявлення складних загроз у мережі. У той же час Angry IP Scanner більш орієнтований на простоту використання та не потребує глибоких знань командного рядка для проведення базового сканування. Ще однією перевагою Nmap над Angry IP Scanner є те що Nmap має модулі які дозволяють проводити певні атаки.

Порівняльний аналіз показав, що обидва інструменти ефективно виконують свої завдання, проте їх доцільно використовувати на різних етапах тестування. Angry IP Scanner підходить для початкової інвентаризації мережі, тоді як Nmap є потужним інструментом для детального аналізу безпеки та пошуку вразливостей. Використання обох інструментів у комплексі дозволяє отримати повнішу картину стану безпеки IoT-пристроїв та підвищує надійність результатів дослідження.

3.3. Збір інформації про сервіси.

Сканування портів для визначення сервісів відноситься до етапу збору інформації, а саме активна розвідка. Цей етап дозволяє отримати детальну інформацію про відкриті порти, активні сервіси та їхні версії, що допомагає визначити потенційні вразливості та точки входу для атаки. Зазвичай для сканування використовуються інструменти на кшталт Nmap, які дозволяють виконати як поверхневе, так і глибоке дослідження мережевих ресурсів.

Під час сканування визначаються сервіси, що працюють на цих портах, їхні версії та конфігурації. Наприклад, відкриті порти для HTTP, FTP, SSH чи Telnet можуть вказувати на можливі слабкі місця у веб-інтерфейсах або механізмах автентифікації пристрою. Важливо також виконувати перевірку на наявність

відомих вразливостей для конкретних версій сервісів, що дозволяє отримати більш повну картину можливих ризиків.

Грамотно проведене сканування допомагає сформувати стратегію подальшого тестування та забезпечує розуміння того, які механізми захисту необхідно впровадити для мінімізації загроз.

На цьому етапі було просканово два хости: 192.168.0.198 і 192.168.0.197, оскільки інші пристрої перестали відповідати на запити, це може свідчити про блокування вхідних запитів через механізм безпеки, пристрій було вимкнено або пристрій перестав працювати.

На хості 192.168.0.180 було просканово єдиний відкритий порт, tcp/5555, на якому працює сервіс, що, ймовірно, є частиною Android Debug Bridge (ADB). Сервіс повернув дані про пристрій, включаючи назву моделі (X96max) і функції (stat_v2, cmd, shell_v2), що підтверджує його належність до ADB.

Наявність відкритого порту 5555 вказує на потенційну вразливість, оскільки ADB дозволяє виконувати команди на пристрої через мережу. Це створює ризик несанкціонованого доступу, особливо якщо автентифікація не налаштована.

Наступним було просканово хост 192.168.0.197 і було перевірено сервіси на трьох відкритих портах: 80/tcp, 554/tcp, та 8086/tcp.

На порту 80/tcp працює веб-сервіс, але його точна версія не визначена. Було виконано кілька перевірок на вразливості, зокрема на stored XSS, CSRF та DOM-based XSS, але жодна з цих вразливостей не була виявлена. Також спроба виконати скрипти для виявлення вразливості CVE-2014-3704 та перевірки на ASP.NET debug mode завершилася помилкою виконання, що може свідчити про нестабільність або некоректну конфігурацію сервісу.

Порт 554/tcp відповідає протоколу RTSP (Real-Time Streaming Protocol), який зазвичай використовується для передачі потокового відео, наприклад, у IP-камерах або медіа-серверах. Точна версія сервісу не була визначена, але відкритий RTSP може потенційно вказувати на пристрій для відеоспостереження або потоковий сервер.

На порту 8086/tcp працює невизначений сервіс, який Nmap позначив як d-s-n?. Це може бути нестандартний веб-сервіс або інтерфейс для керування пристроєм. Відкритий порт 8086 часто використовується для баз даних, зокрема InfluxDB, або для панелей управління IoT-пристроїв.

Три відкриті порти вказують на активні сервіси, які можуть використовуватися для керування пристроєм або потоковою передачею даних.

3.4. Аналіз потенційних загроз

Аналіз потенційних загроз є важливим етапом не тільки забезпечення безпеки IoT-пристроїв, а й нормального функціонування бізнесу, оскільки дозволяє заздалегідь виявити можливі вектори атак і підготуватися до їх наслідків. Розуміння загроз допомагає формувати ефективну стратегію реагування, що включає як профілактичні заходи, так і план дій на випадок компрометації. Оцінка ризиків, пов’язаних із конкретними вразливостями, дозволяє прогнозувати ймовірні сценарії атак і визначати їхній вплив на працездатність пристрою, конфіденційність даних та загальну безпеку мережі. Дослідження показують, що вразливості IoT-систем часто пов’язані з недостатнім захистом автентифікації, незашифрованим з’єднанням та слабким контролем доступу, що створює значні ризики для конфіденційності та цілісності даних [35].

Завдяки аналізу загроз можна виявити слабкі місця в конфігурації пристроїв, незахищені сервіси або вразливості у програмному забезпеченні, які можуть бути використані зловмисниками для проникнення в систему. Кожна виявлена загроза повинна бути детально досліджена для того, щоб оцінити рівень ризику, ймовірність реалізації атаки та можливі наслідки для системи. Наприклад, відкриті порти та незахищені сервіси можуть стати точками входу для несанкціонованого доступу, а розкриття конфіденційної інформації може призвести до витоку даних або фінансових втрат.

Окрім цього, аналіз загроз дозволяє планувати заходи для мінімізації їхнього впливу. Завдяки цьому організації можуть впроваджувати моніторинг підозрілої активності, налаштовувати системи сповіщення про потенційні атаки та розробляти процедури відновлення після інцидентів. Застосування сучасних технологій моніторингу мережевої безпеки дозволяє вчасно ідентифікувати аномальну активність, що є критичним для захисту IoT-пристроїв від потенційних загроз і атак [34]. Заздалегідь підготовлений план реагування допомагає швидко локалізувати загрозу, мінімізувати її наслідки та відновити нормальну роботу системи.

Також, як зазначено у дослідженні, впровадження систем виявлення мережевих атак на основі методів машинного навчання дозволяє ефективно ідентифікувати такі загрози, як DDoS-атаки, ботнети та атаки на вебсервіси, забезпечуючи своєчасне реагування на потенційні загрози та мінімізацію їхніх наслідків [33]

На першому хості(192.168.0.198) було виявлено відкритий порт 5555/tcp, на якому працює сервіс, ймовірно, пов’язаний з Android Debug Bridge (ADB). Цей сервіс надає можливість віддаленого доступу до пристрою для виконання команд і налагодження, що створює низку потенційних загроз.

- несанкціонований віддалений доступ: відкритий порт 5555 для ADB без належного захисту дозволяє зловмиснику підключатися до пристрою та отримати повний контроль над ним.
- виконання довільного коду: ADB підтримує виконання команд на пристрої.
- інформаційне розкриття: під час сканування було отримано дані про пристрій, такі як назва моделі (X96max) та функції (stat_v2, cmd, shell_v2).
- скомпрометована конфіденційність: якщо пристрій використовується для обробки або зберігання конфіденційних даних, відкритий ADB дозволяє зловмиснику викрасти цю інформацію або перехопити дані, що передаються через мережу.

– формування ботнету: пристрої з відкритим ADB-портом часто стають цілями для ботнет-атак, подібних до Mirai.

Таким чином, відкритий порт 5555/tcp із активним ADB-сервісом є значним ризиком для безпеки пристрою, оскільки створює можливості для несанкціонованого доступу, виконання шкідливих команд та викрадення даних.

Сканування хоста 192.168.0.197 виявило відкриті порти 80/tcp, 554/tcp, та 8086/tcp, що вказує на активні сервіси, пов’язані з веб-доступом та потоковою передачею даних. Ці відкриті порти можуть створити потенційні загрози для безпеки пристрою при їх неправильному налаштуванні.

На порту 80/tcp працює веб-сервіс, але його версія не була визначена. Спроби автоматизованого сканування на наявність вразливостей, таких як stored XSS, DOM-based XSS, та CSRF, не виявили загроз, але скрипти для перевірки на вразливість CVE-2014-3704 та ASP.NET debug mode не вдалося виконати. Це може свідчити про нестабільність сервісу або специфічні налаштування, що ускладнюють виявлення. Відкритий порт 80 є типовою точкою входу для веб-атак, таких як SQL-ін'єкції, XSS, або атаки на автентифікацію.

Порт 554/tcp відповідає протоколу RTSP (Real-Time Streaming Protocol), що часто використовується для IP-камер та потокових медіа-серверів. Незахищений RTSP може дозволяти зловмиснику переглядати відеопотоки, перехоплювати конфіденційні дані або здійснювати атаки типу Man-in-the-Middle (MitM) для підміни відеопотоку.

На порту 8086/tcp працює невизначений сервіс, який може бути пов'язаний із базами даних або веб-інтерфейсами управління. Порт 8086 часто використовується для InfluxDB або інших систем для збору та аналізу даних. Незахищений доступ до цього порту може призвести до витоку даних або дозволити зловмиснику змінювати конфігурації системи.

Комбінація відкритих портів 80, 554 і 8086 створює ризик для конфіденційності та цілісності даних, а також можливість несанкціонованого доступу до пристрою чи його функцій.

3.5. Аналіз можливих наслідків атак

На хості 192.168.0.198 було виявлено лише один відкритий порт – 5555. Судячи з інформації отриманої з допомогою Nmap, цей порт пов’язаний із Android Debug Bridge (ADB)**.** Цей сервіс надає можливість виконання команд на пристрої та доступу до його файлової системи. Зловмисник може використати відкритий ADB для підключення до пристрою без автентифікації. Це дозволяє отримати повний контроль над пристроєм, виконувати довільні команди, завантажувати та видаляти файли, а також вносити зміни до налаштувань системи. Наслідком може бути повна компрометація пристрою та витік конфіденційних даних.

Також ADB може бути використано зловмисником для завантаження та встановлення шкідливих програм, такі як бекдори, кейлогери чи програми для майнінгу криптовалюти. Це може призвести до постійного контролю над пристроєм і його використання в ботнет-мережах для проведення DDoS-атак або інших злочинних дій.

Якщо пристрій зберігає персональні дані або інші чутливі відомості, зловмисник може їх викрасти. Це може спричинити фінансові втрати, порушення конфіденційності або компрометацію інших систем у мережі.

Хост 192.168.0.197 має більше відкритих портів, а значить більше потенційних точок входу в систему. Веб-сервіс на порту 80 може бути вразливим до атак типу SQL-ін'єкція**,** Cross-Site Scripting (XSS) або Cross-Site Request Forgery (CSRF) та багатьох інших атак якщо не правильно сконфігурований або застарілий. Один з найбільших недоліків веб-сервісів на 80 порті це відсутність шифрування трафіку. Завдяки цьому будь хто в мережі може перехоплювати незашифрований трафік тим самим отримуючи чутливі дані. У разі успішної атаки зловмисник може отримати доступ до конфіденційних даних, змінювати веб-сторінки або виконувати дії від імені користувача. Наслідками можуть бути витік даних, злам облікових записів або пошкодження веб-додатка. Протокол RTSP використовується для потокової передачі відео. Зловмисник може

здійснити атаку для несанкціонованого перегляду відеопотоків або перехоплення даних. Це призводить до порушення конфіденційності, витоку відеоматеріалів та можливого втручання у системи відеоспостереження. Порт 8086 часто використовується базами даних, такими як InfluxDB, або веб-інтерфейсами для керування пристроями. Незахищений сервіс на цьому порту може дозволити зловмиснику отримати доступ до даних або внести несанкціоновані зміни у налаштування системи. Наслідками можуть бути викрадення даних, модифікація записів або повне виведення сервісу з ладу.

3.6. Експлуатація знайдених вразливостей та рекомендації для підвищення рівня безпеки.

У цьому розділі буде детально розглянуто процес компрометації IP-камери на основі виявлених вразливостей під час попереднього сканування. Вибір саме IP-камери як об'єкта атаки є обґрунтованим через те, що подібні пристрої часто стають мішенями для кіберзлочинців і були основною складовою у відомих ботнетах, таких як Mirai. Неналежний захист IP-камер може призвести до критичних наслідків, включаючи несанкціоноване спостереження, витік конфіденційних даних та використання пристрою для подальших атак.

На основі отриманих результатів сканування буде продемонстровано етапи проведення атаки на IP-камеру, а також надано рекомендації для запобігання подібним інцидентам у майбутньому.

В попередніх етапах тестування мережі, було виявлено декілька IoT пристроїв, зокрема IP-камери. Ціллю атаки було обрано саме IP-камеру, оскільки саме айпі камери складали більшу частину найбільшого в історії ботнету під назвою Mirai-ботнет, отже забезпечення надійного саме цих пристроїв є найбільш критичним. Окрім того, камери в залежності від того де вони встановленні можуть надати зловмиснику дуже цінну і чутливу інформацію.

На етапі сканування відкритих портів, було виявлено що на хості 192.168.0.197 відкритий порт 80, що свідчить про наявність веб-інтерфейсу який

потенційно може бути проексплуатований для отримання несанкціонованого доступу. При спробі підключення до камери через веб-інтерфейс у браузері з’явилася пропозиція завантажити програмне забезпечення для управління пристроєм. Це програмне забезпечення є стандартним для багатьох моделей камер і слугує інтерфейсом для підключення та налаштування пристрою. Сторінка веб-інтерфейсу цієї камери зображено на рисунку 3.1.

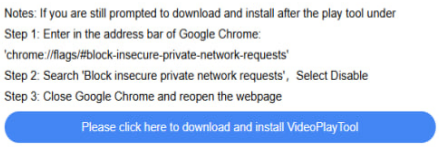

Рисунок 3.1 – Веб-інтерфейс IP-камери

Завантаження та встановлення цього програмного забезпечення пройшло без будь-яких перевірок автентичності або додаткових заходів безпеки, що вже вказує на потенційні загрози, пов’язані з відсутністю контролю доступу на цьому етапі.

Після встановлення програмного забезпечення система запропонувала увійти до існуючого облікового запису або створити новий. Процес створення облікового запису не передбачав жодної перевірки прав доступу чи автентичності користувача, що дозволило створити новий обліковий запис і тим самим отримати доступ до функцій камери.

Під час першої спроби підключення до камери було необхідно ввести певні дані для автентифікації: ім'я пристрою(необхідно придумати самому), серійний

номер камери, логін та пароль. Серійний номер був легко доступний на самому пристрої, оскільки камера не мала фізичного захисту від несанкціонованого доступу. Таке розміщення серійного номера на видному місці створює значний ризик компрометації пристрою у випадку фізичного доступу до нього зловмисника. Інтерфейс входу в камеру зображено на рисунку 3.2.

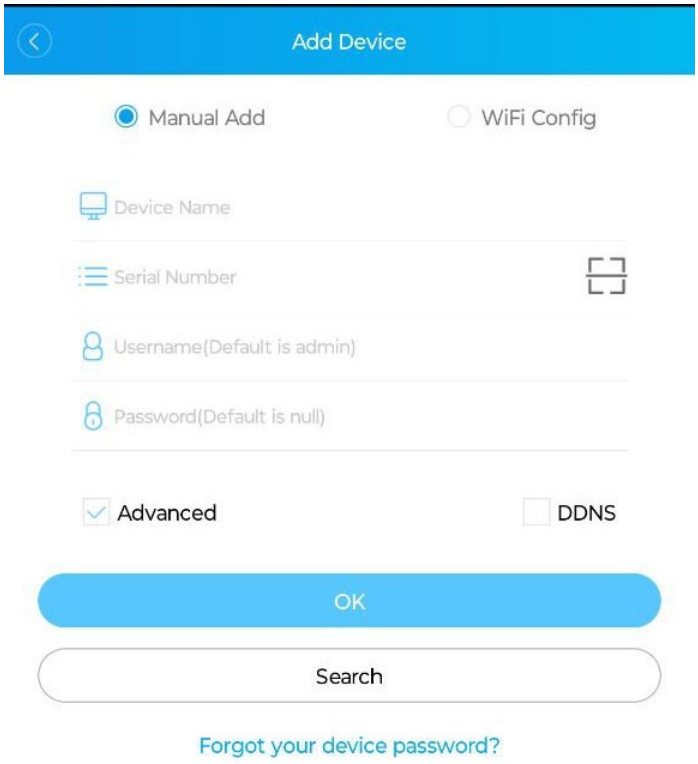

Рисунок 3.2 – Інтерфейс логіну IP-камери

Варто також зазначити, що веб-інтерфейс автентифікації передбачав використання стандартних налаштувань для логіна та пароля. У відповідних полях для введення логіна та пароля були вказівки "default is admin" для логіна та "default is null" для пароля, що означало відсутність пароля за замовчуванням і використання ненадійних, стандартних облікових записів. Введення цих стандартних даних дозволило успішно авторизуватись у системі камери без необхідності підбору складних комбінацій або застосування додаткових інструментів для злому пароля.

Після успішного проходження автентифікації було отримано повний доступ до функцій камери, включаючи перегляд відеопотоку в реальному часі та

можливість зміни налаштувань пристрою. Цей факт підтверджує, що камера була скомпрометована внаслідок комбінації кількох критичних вразливостей: наявності відкритого веб-інтерфейсу без захисту, доступності серійного номера на корпусі пристрою та використання стандартних налаштувань автентифікації.

Таким чином, компрометація IP-камери демонструє типовий сценарій атаки на IoT-пристрої, коли зловмисник може скористатися як технічними вразливостями, так і недоліками у фізичному захисті пристрою. У цьому випадку ключовими факторами успіху атаки стали відсутність належного контролю доступу, можливість легко отримати критичні дані для автентифікації та недбале управління паролями, що призвело до повного доступу до функцій камери без значного прикладення зусиль зі сторони зловмисника.

В процесі аналізу вразливостей IP-камери було виявлено низку суттєвих недоліків, які відповідають категоріям, визначеним у OWASP IoT Top 10. Одним із найбільш критичних недоліків є недостатній контроль автентифікації. Пристрій використовував стандартний логін admin і відсутність пароля за замовчуванням, що значно спрощувало несанкціонований доступ. Цей недолік підпадає під категорію A1: Weak, Guessable, or Hardcoded Passwords. Використання стандартних паролів, які легко вгадати, залишається поширеною проблемою серед IoT-пристроїв. Окрім того що пристрій використовував стандартні облікові дані і давав про це підказку, також не було передбачено жодного захисту від атак грубої сили.

Важливим аспектом вразливості також є незахищений веб-інтерфейс камери, доступний через порт 80, що використовує незашифроване з’єднання за допомогою протоколу HTTP. Це дозволяє зловмиснику потенційно перехоплювати дані під час їх передачі між пристроєм та користувачем, що відповідає категорії A3: Insecure Ecosystem Interfaces у класифікації OWASP IoT Top 10. Відсутність шифрування відкриває можливості для атак Man-in-the-Middle та інших методів перехоплення. Крім того, незахищена процедура завантаження програмного забезпечення з веб-інтерфейсу підвищує ймовірність компрометації пристрою через інфікування шкідливим кодом.

Фізична безпека пристрою також викликає значні занепокоєння. Серійний номер камери був розташований на її корпусі без будь-якого захисту, що дає можливість зловмиснику легко отримати необхідну для автентифікації інформацію. Це свідчить про недоліки у фізичному захисті пристрою, що узгоджується з категорією A10: Lack of Physical Hardening. У випадку фізичного доступу до пристрою, отримання критичних даних, таких як серійний номер, стає тривіальним завданням.

Ще одним вразливим місцем є відсутність належного контролю доступу до функціоналу веб-інтерфейсу. Можливість створення облікового запису без належної перевірки автентичності користувача демонструє слабкий контроль над процесом управління доступом, що відповідає категорії A2: Insecure Network Services. Це дозволяє зловмисникам створювати облікові записи для подальшого несанкціонованого доступу до камери.

Для усунення вказаних недоліків необхідно запровадити надійну автентифікацію, що передбачає обов’язкову зміну стандартного пароля під час першого підключення до пристрою. Пароль повинен бути складним та містити комбінацію великих і малих літер, цифр і спеціальних символів. Крім того, впровадження двохфакторної автентифікації допоможе підвищити рівень захисту. З метою забезпечення конфіденційності передачі даних необхідно перевести веб-інтерфейс на захищений протокол HTTPS та впровадити використання надійних SSL/TLS-сертифікатів. Це дозволить захистити дані від перехоплення під час передачі.

Важливим заходом є покращення фізичної безпеки камери шляхом приховування серійного номера або його розміщення у місцях, недоступних для сторонніх осіб. Також слід використовувати додаткові захисні кожухи для ускладнення фізичного доступу до пристрою. Посилення контролю доступу до веб-інтерфейсу передбачає обмеження можливості створення нових облікових записів лише адміністративними користувачами та впровадження функції блокування IP-адрес після кількох невдалих спроб входу.

Проведене дослідження IoT-пристроїв у домашній мережі показало наявність критичних вразливостей, що можуть бути потенційно використані зловмисниками для компрометації IoT-пристроїв. Однією з основних проблем, виявлених під час сканування, є недостатній рівень автентифікації на більшості пристроїв. Більшість пристроїв використовували стандартні облікові дані або не мали паролів взагалі, що спрощує несанкціонований доступ.

Аналіз також виявив використання незашифрованих протоколів для передачі даних, таких як HTTP. Відсутність шифрування дозволяє перехоплювати дані, що передаються між користувачами та пристроями, створюючи умови для атак Man-in-the-Middle. Це стосується не лише IP-камер, але й інших пристроїв у мережі, таких як телевізори та інші елементи інфраструктури розумного дому.

Фізичний захист IoT-пристроїв також залишається на низькому рівні. Доступ до ідентифікаційної інформації, такої як серійні номери або інші конфіденційні дані, часто не захищений належним чином. Зловмисник, який має фізичний доступ до пристрою, може легко отримати критичні дані для автентифікації або налаштування пристрою.

Недостатність налаштувань безпеки на рівні конфігурації пристроїв також була виявлена як значний недолік. Пристрої часто дозволяють створювати облікові записи або змінювати параметри без належного контролю доступу. Це відкриває можливості для створення бекдорів або встановлення несанкціонованого контролю над пристроями.

Загалом аналіз продемонстрував, що більшість пристроїв у мережі страждають від типових проблем безпеки, характерних для IoT-середовищ. Відсутність надійної автентифікації, використання незашифрованих протоколів передачі даних та слабкий фізичний захист значно підвищують ризик компрометації. Усі ці вразливості можуть бути використані як окремо, так і в комбінації для проведення комплексних атак.

Для підвищення рівня безпеки необхідно впровадити низку заходів, включаючи використання надійних паролів, шифрування даних за допомогою

HTTPS та TLS, посилення контролю доступу та забезпечення фізичної безпеки пристроїв. Регулярне оновлення прошивки та обмеження доступу до інтерфейсів конфігурування допоможуть мінімізувати ризики несанкціонованого доступу. Проведення періодичних сканувань та аудитів мережі дозволить виявляти нові загрози та оперативно реагувати на них, забезпечуючи стабільний рівень безпеки IoT-інфраструктури.

Ефективність захисту IoT-пристроїв значною мірою залежить від стійких криптографічних алгоритмів, що забезпечують захист даних від несанкціонованого доступу. Як зазначено у дослідженні, використання алгоритмів для генерації нелінійних підстановок, таких як алгоритм імітації відпалу, дозволяє підвищити криптографічну стійкість шляхом оптимізації замін, що є важливим аспектом для забезпечення конфіденційності та цілісності даних[32].

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Війна стала масштабним структурним шоком як для економіки України, так і для кожного регіону держави. Неможливо спрогнозувати терміни і наслідки військової агресії, водночас стратегічні цілі держави та окремих регіонів потребують коригування відповідно до умов воєнного часу і післявоєнної відбудови.

В умовах війни необхідний перегляд усталених підходів як до стратегічного планування, так і до розв’язання гострих соціально-економічних, гуманітарних і безпекових проблем розвитку держави на всіх рівнях ієрархії управління, включно з регіональним.

Можлива війна на виснаження потребує від України та її регіонів проведення обачної економічної політики вже зараз. Міжнародні резерви мають використовуватися економно, а бюджетні ресурси необхідно спрямовувати на фінансування військових потреб і підтримку життєдіяльності в умовах воєнного стану.

З огляду на перебіг військових дій, спричинених агресією російської федерації, територію України можна поділити на тимчасово окуповані ворогом, звільнені після окупації, прифронтові з високою ймовірністю загрози окупації, фронтові, на яких тривають бойові дії, та регіони, що виконують функції глибокого тилу.

Наслідки збройної агресії російської федерації найбільше відбилися на реальному секторі економіки країни, зокрема на підприємствах, що розташовані на тимчасово окупованих або звільнених після окупації територіях, а також у регіонах з високою ймовірністю загрози окупації, які забезпечували значну частину внутрішнього промислового виробництва та експорту.

Завданням тилових регіонів є збереження стратегічно важливих виробництв і робочих місць, підтримка діяльності релокованих підприємств із територій, де ведуться активні бойові дії, а також підтримка експортно орієнтованих підприємств і виробників соціально значущих товарів та товарів військового призначення. Необхідно стимулювати перехід до виробництва продукції військового призначення.

В умовах воєнного часу на першому етапі йдеться про реалізацію заходів, спрямованих на максимальне збереження людей та підприємств, виконання гуманітарних місій. Масштаб і успіхи плану реконструкції на цьому етапі залежать від того, наскільки українці, економіка та інституції будуть врятовані від війни. Щоб мінімізувати збитки, Україна та союзники мають структурувати економіку воєнного часу згідно з безпековими ризиками.

На цій стадії Львівщина, як відносно безпечний регіон, виконує роль «глибокого тилу» країни: надає допомогу переміщеним підприємствам, формує програми зайнятості для внутрішньо переміщених осіб, забезпечує технічну підтримку логістики та цифрової мобільності, підтримує транспортні коридори для ввезення гуманітарної допомоги, а також для імпорту й експорту. Також регіон впроваджує будівництво житла для внутрішньо переміщених осіб і максимально зберігає свій економічний потенціал.

Одночасно тилові регіони надають допомогу прифронтовим та фронтовим регіонам у вигляді гуманітарної допомоги (продукти, пальне, ліки), технічної допомоги в евакуації виробництва (де це можливо або доцільно), а також логістичної підтримки для забезпечення зв’язку цих регіонів із рештою країни.

Як тиловий регіон в умовах воєнного стану, Львівщина має також зосередити зусилля на забезпеченні заходів національного спротиву, антитерористичному захисті, належному функціонуванні систем оповіщення та укриттів.

Ризиком цього періоду є затягування та подальша ескалація бойових дій, масштабна руйнація інфраструктури через ракетні удари або окупація регіону.

Стійкість роботи промислового об’єкта (незалежно від форми власності) визначається його здатністю випускати продукцію в запланованому обсязі навіть в умовах надзвичайних ситуацій мирного і воєнного часу. У разі слабких або середніх руйнувань та порушення коопераційних зв’язків підприємство має відновити виробництво в мінімальні терміни.

Здатність підприємства приладобудівної галузі випускати продукцію залежить від захисту і нормального функціонування чотирьох основних елементів сучасного виробництва:

– виробничого персоналу (робітники та службовці);
– будівель і споруд із технологічним устаткуванням;
– системи постачання енергією, водою, паливом, устаткуванням і ремонтною базою;
– системи виробничих і кооперативних зв’язків із іншими об’єктами.
– стійкість роботи підприємства приладобудівної галузі в умовах надзвичайних ситуацій визначається такими факторами:
– надійністю захисту робітників і службовців від усіх вражаючих факторів зброї масового ураження;
– здатністю інженерно-технічного комплексу протистояти вражаючим факторам ядерного вибуху;
– надійністю системи постачання об’єкта необхідними ресурсами (сировиною, паливом, комплектуючими виробами, електроенергією, водою, газом тощо);
– захищеністю від вторинних вражаючих факторів (пожеж, вибухів, затоплень, зараження території отруйними речовинами);
– стійкістю та безперервністю керування виробництвом і цивільною обороною;
– готовністю до проведення рятувальних та відновлювальних робіт.

Перераховані фактори визначають основні способи підвищення стійкості роботи всіх підприємств у надзвичайних ситуаціях. А саме:

- забезпечення надійного захисту персоналу від впливу зброї масового ураження;
- захист виробничих фондів від первинних і вторинних вражаючих факторів;
- підвищення ефективності управління виробничими процесами;
- забезпечення стабільного постачання всіх необхідних ресурсів для виготовлення продукції;
- завчасна підготовка до відновлення виробничих процесів після пошкоджень.

Для забезпечення максимальної стійкості роботи підприємств під час надзвичайних ситуацій необхідно враховувати як технічні, так і організаційні аспекти підготовки. Впровадження автоматизованих систем моніторингу дозволяє в реальному часі відстежувати стан будівель, обладнання та інфраструктури. Ці системи здатні фіксувати навіть незначні пошкодження та своєчасно інформувати відповідні служби для оперативного реагування. Крім того, використання технології цифрових двійників підприємства допомагає створити віртуальну модель виробництва, що дозволяє прогнозувати можливі сценарії руйнувань і розробляти заходи для мінімізації їхніх наслідків. Це підвищує готовність підприємства до потенційних загроз та забезпечує більш швидке відновлення виробничих процесів.

Системи резервного копіювання даних також є критично важливими для стійкої роботи підприємства в умовах надзвичайних ситуацій. Надійне збереження інформації та можливість її швидкого відновлення дозволяють зменшити час простою та мінімізувати фінансові збитки. У випадку з приладобудівними підприємствами особливу увагу слід приділяти захисту високоточного обладнання. Необхідно розробляти спеціальні укриття для верстатів та технологічного устаткування, які забезпечать додаткову стійкість до ударних хвиль і світлового випромінювання. Окрім цього, важливо передбачити можливість швидкого демонтажу та евакуації найціннішого обладнання для його подальшого використання на резервних потужностях.

Дублювання критичних виробничих процесів на інших підприємствах або в регіонах, менш схильних до загроз, є дієвим способом забезпечення безперервності виробництва. Це дозволяє продовжувати випуск продукції навіть у випадку руйнування основного виробничого майданчика. Використання мобільних модульних систем для тимчасової організації виробничих процесів може стати важливим інструментом для швидкого відновлення діяльності підприємства. Такі системи можна оперативно розгорнути на нових локаціях і відновити виробництво критично важливої продукції.

Підготовка персоналу до дій у надзвичайних ситуаціях також є важливим аспектом підвищення стійкості підприємства. Регулярні навчання та тренування допомагають працівникам краще розуміти порядок дій під час НС. Проведення інтерактивних симуляцій дозволяє відпрацювати різні сценарії та підвищити рівень готовності. Особливу увагу слід приділяти керівному складу, адже від їхніх швидких та ефективних рішень залежить подальша стабільність роботи підприємства. Розробка чітких алгоритмів для керівників дозволяє мінімізувати час на прийняття важливих рішень під час кризи.

Ефективна координація з місцевими органами влади та державними службами є необхідною умовою для успішного реагування на надзвичайні ситуації. Співпраця з рятувальними службами, медичними установами та правоохоронними органами забезпечує своєчасну підтримку та необхідну допомогу. Участь у регіональних програмах підвищення безпеки допомагає підприємствам обмінюватися досвідом, ресурсами та вдосконалювати свої стратегії реагування. Комплексний підхід до підготовки, який включає технічні інновації, навчання персоналу та ефективну взаємодію з державними структурами, дозволяє підприємствам мінімізувати ризики та швидко відновлювати свою діяльність у найскладніших умовах.

4.2. Безпека в надзвичайних ситуаціях

Забезпечення безпеки життєдіяльності під час роботи з комп’ютерами та IoT-пристроями є важливим етапом для збереження здоров'я та ефективної експлуатації обладнання. У сучасному світі цифрові технології глибоко інтегровані у повсякденне життя, а комп’ютери, розумні пристрої та IoT-системи стають невід’ємною частиною як домашнього середовища, так і виробничих процесів. Однак робота з такими пристроями передбачає не лише інформаційну безпеку, а й фізичну безпеку, оскільки вони містять електричні компоненти, датчики та механізми, що можуть становити потенційну загрозу при неправильному використанні.

Основними ризиками є ураження електричним струмом, перегрів пристроїв, що може призвести до опіків або загоряння, а також травмування через роботу з рухомими частинами пристроїв, як-от роботи-пилососи чи дрони. Крім того, під час обслуговування або ремонту електронних компонентів є ризик пошкодження обладнання через статичну електрику або неправильне підключення.

Дотримання правил техніки безпеки допомагає мінімізувати ці ризики та забезпечує стабільну й безпечну роботу обладнання. Це включає правильне поводження з електричними проводами та елементами живлення, використання засобів індивідуального захисту, дотримання безпечних умов роботи та регулярну перевірку справності пристроїв. Розуміння та впровадження цих заходів дозволить уникнути аварійних ситуацій та забезпечить тривалу й безпечну експлуатацію комп’ютерів та IoT-пристроїв.

Продукція яка має маркування відповідності Європі (CE), розроблена та протестована на стійкість до міжнародних стандартів електростатичного розряду (ESD). Ці продукти були розроблені та визначені як такі, що відповідають стандартним рівням для ESD. Однак можуть виникнути ситуації, такі як низький рівень вологості, які можуть посилити виникнення ОСР.

Електростатичний розряд (ESD) може пошкодити електронні компоненти всередині комп'ютера. За певних умов ESD може накопичуватися на тілі або

об'єкті, наприклад, периферійному пристрої, а потім розтікатися в інший об'єкт. Щоб запобігти пошкодженню електростатичними розрядами, необхідно розрядити статичну електрику з тіла, перш ніж взаємодіяти з будь-якими внутрішніми електронними компонентами комп'ютера.

Для того щоб захиститися від електростатичного розряду та розрядити статичну електрику з тіла, необхідно торкнутись предмета з металевим заземленням, перш ніж взаємодіяти з будь-чим електронним. Під час підключення периферійного пристрою (включаючи кишенькових цифрових помічників) до комп'ютера потрібно завжди заземлити як користувача, так і периферійний пристрій, перш ніж підключати його до комп'ютера. Крім того, працюючи за комп'ютером, необхідно періодично торкатись предмета з металевим заземленням, щоб видалити будь-який статичний заряд, який міг накопичитися у тілі.

Також можна вжити таких заходів, щоб запобігти пошкодженню від електростатичного розряду:

- під час розпакування чутливого до статичної електрики компонента з транспортної коробки не можна виймати компонент з антистатичного пакувального матеріалу, доки компонент не буде готовий до встановлення. Перш ніж розгорнути антистатичний пакет, необхідно усунути статичну електрику з тіла.
- транспортувати чутливий компонент можна тільки у антистатичному контейнері або упаковці.
- обробляти електростатичні чутливі компоненти можна тільки в статично безпечній зоні. Якщо можливо, потрібно використовувати антистатичні підлогові накладки та накладки для робочого столу.
- для того щоб захистити комп'ютер від можливих пошкоджень і забезпечити особисту безпеку, слід слідувати наступним правилам:
- обладнання має стояти на твердій рівній поверхні. Також потрібно залишити мінімум 10,2 см (4 дюйми) вільного простору на всіх вентильованих сторонах комп'ютера, щоб забезпечити потік повітря,

необхідний для належної вентиляції. Обмеження потоку повітря може пошкодити комп'ютер або спричинити пожежу.

- слід уникати складання обладнання та розміщення його так близько одне до одного, щоб воно піддавалося повторній циркуляції або впливу попередньо нагрітого повітря.
- слід переконатися, що на кабелях обладнання нічого не лежить і що кабелі не розташовані в місцях, де на них можна наступити або спіткнутися.
- необхідно перевірити, чи всі кабелі підключені до відповідних роз'ємів. Деякі роз'єми мають схожий зовнішній вигляд і можуть вводити в оману (наприклад, телефонний кабель не слід підключати до мережевого роз'єму).
- не варто розміщувати пристрій у закритому настінному блоці або на м'яких тканинних поверхнях, таких як ліжко, диван чи килим.
- пристрій слід тримати подалі від радіаторів і джерел тепла.
- обладнання необхідно зберігати подалі від надзвичайно високих або низьких температур для забезпечення роботи в допустимому діапазоні.
- заборонено вставляти будь-які предмети у вентиляційні отвори обладнання, щоб уникнути пожежі або ураження електричним струмом через коротке замикання внутрішніх компонентів.
- обладнання не слід використовувати у вологих місцях, таких як ванна, раковина, басейн або вологий підвал.
- не рекомендується користуватися обладнанням, що працює від змінного струму, під час грози. Можна використовувати пристрої на акумуляторі за умови відключення всіх кабелів.
- заборонено проливати їжу або рідини на обладнання.
- перед очисткою обладнання необхідно від'єднати його від електричної розетки. Для очистки слід використовувати м'яку тканину, змочену водою. Не варто застосовувати рідини або аерозольні очищувачі, що містять легкозаймисті речовини.

– РК-екран ноутбука або дисплей монітора слід чистити м'якою чистою тканиною та водою. Воду слід наносити на тканину, після чого протирати дисплей у напрямку зверху вниз. Важливо швидко видаляти вологу, щоб уникнути пошкодження дисплея. Комерційні засоби для миття вікон використовувати не рекомендується.

Після роботи за комп'ютером:

– щоб уникнути потенційної небезпеки ураження електричним струмом, не слід підключати або від'єднувати кабелі, а також виконувати технічне обслуговування чи зміну конфігурації обладнання під час грози.
– рекомендується зберегти та закрити всі відкриті файли, а також закрити всі відкриті програми.
– необхідно вимкнути комп'ютер через меню: «Пуск > Живлення > Завершити роботу».
– слід від'єднати комп'ютер та всі підключені пристрої від електричних розеток.
– слід від'єднати від комп'ютера всі мережеві та периферійні пристрої, такі як клавіатура, миша та монітор.
– відеокарту та оптичний диск необхідно від'єднати від комп'ютера, якщо це можливо.
– перед роботою з компонентами всередині комп'ютера слід заземлитися. Для цього рекомендується використовувати ремінь заземлення або періодично торкатися нефарбованої металевої поверхні, наприклад, металу на задній панелі комп'ютера.
– для уникнення пошкоджень важливо переконатися, що робоча поверхня рівна і чиста.
– слід поводитися з компонентами обережно. Не варто торкатися контактів на карті; необхідно тримати картку за краї або монтажний кронштейн.
– під час від'єднання кабелів потрібно тягнути за роз'єм або фіксуючий язичок, а не за сам кабель.

Перед початком роботи за комп'ютером:

– необхідно перевірити та закрутити всі гвинти. Слід переконатися, що всередині комп'ютера не залишилося незакріплених деталей.
– слід підключити всі зовнішні пристрої та периферію (клавіатура, миша, монітор тощо), які були від'єднані під час технічного обслуговування.
– варто встановити на місце всі компоненти, такі як відеокарта, жорсткі диски та інші деталі, які були зняті під час роботи.
– потрібно підключити комп'ютер та всі периферійні пристрої до електричних розеток.
– необхідно увімкнути комп'ютер і перевірити, чи все працює коректно.

Загальні вказівки з енергетичної безпеки:

– перед підключенням обладнання необхідно перевірити номінальну напругу на відповідність джерелу живлення.
– слід переконатись, що пристрої розраховані на роботу з напругою мережі змінного струму, доступною у цільовому регіоні.
– не слід підключати кабелі живлення до розетки, якщо кабель пошкоджено.
– щоб уникнути ураження струмом, кабелі живлення слід підключати до заземлених розеток.
– під час використання подовжувача необхідно стежити, щоб загальний номінальний струм не перевищував допустимий.
– подовжувачі необхідно підключати безпосередньо до настінної розетки, а не до інших подовжувачів.
– під час відключення обладнання слід тримати за вилку, а не за кабель.
– важливо використовувати лише адаптер змінного струму, схвалений для конкретного пристрою.
– адаптер змінного струму слід розміщувати у провітрюваному місці та уникати його накривання предметами.
– адаптер змінного струму може нагріватися під час нормальної роботи комп'ютера. Необхідно враховувати це під час або відразу після роботи з адаптером.

– рекомендується покласти адаптер на підлогу або стіл так, щоб було видно зелене світло. Це буде служити попередженням, якщо адаптер випадково вимкнеться через зовнішній вплив. Якщо з будь-якої причини зелене світло згасне, потрібно від'єднати шнур змінного струму від стіни на десять секунд, а потім знову підключити кабель живлення.
– слід уникати використання адаптера, який має видимі ознаки пошкодження.

ВИСНОВКИ

У ході дослідження було проаналізовано загрози та вразливості, притаманні IoT-пристроям, а також потенційні методи тестування на проникнення, що дозволяють їх виявити. Завдяки проведеній атаці, видно, наскільки серйозними можуть бути наслідки недостатнього захисту IoT-систем. Було встановлено, що основними причинами компрометації є слабкі паролі, незахищені інтерфейси, застаріле програмне забезпечення та відсутність сегментації мережі.

Сканування хостів у домашній мережі підтвердило наявність потенційних вразливостей, таких як відкриті порти з активними сервісами для віддаленого доступу (ADB) та веб-інтерфейси на портах 80**,** 554**,** і 8086. Ці сервіси створюють ризики несанкціонованого доступу, витоку конфіденційної інформації та можливості використання пристроїв у ботнет-мережах. Аналіз можливих атак показав, що зловмисники можуть здійснювати як віддалене керування пристроями, так і маніпуляції з даними або відеопотоками.

Загалом дослідження підкреслило важливість регулярного аналізу безпеки IoT-пристроїв та необхідність впровадження комплексного підходу до їх захисту. Навіть у домашніх мережах загрози є реальними та можуть мати серйозні наслідки у випадку успішних атак.

Для підвищення безпеки IoT-пристроїв у домашній мережі з урахуванням загроз, виявлених під час сканування домашньої мережі, слід зосередитися на кількох ключових заходах. Перш за все, необхідно змінити стандартні паролі на надійні та унікальні комбінації для всіх пристроїв, які мають відкриті сервіси віддаленого доступу, такі як ADB на порту 5555. Це допоможе запобігти несанкціонованому доступу та виконанню довільних команд на пристроях.

Важливим кроком є закриття всіх непотрібних портів і вимкнення сервісів, які не використовуються, зокрема сервісу ADB, якщо він не є критично необхідним для роботи пристрою. Відкритий порт 80, що відповідає за веб-доступ, а також порт 554, на якому працює RTSP, слід захистити належною

автентифікацією та шифруванням, щоб уникнути ризиків несанкціонованого перегляду потокового відео або доступу до веб-інтерфейсу.

Оновлення прошивок є важливим заходом для закриття відомих вразливостей у веб-сервісах і потокових протоколах. Регулярне оновлення програмного забезпечення допоможе усунути потенційні ризики, пов'язані з вразливими версіями сервісів на відкритих портах.

Для зменшення ризику несанкціонованого доступу варто розділити мережу на сегменти, створивши окрему підмережу для IoT-пристроїв. Це унеможливить поширення атак на інші критичні пристрої у випадку компрометації одного з них. Також доцільно впровадити моніторинг мережевого трафіку для виявлення аномальних підключень до портів 80, 554, 5555 та 8086. Це дозволить своєчасно реагувати на підозрілу активність і запобігти потенційним атакам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Techtarget. Internet of Things (IoT). URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (дата звернення: 16.10.24, 22:10).

2. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

3. Integrity360. What Is IoT Penetration Testing and Why Do You Need It? URL: https://insights.integrity360.com/what-is-iot-penetration-testing-and-why-do-you-need-it.

4. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

5. Cloudflare. Mirai Botnet. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/.

6. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

7. Fortinet. Command and Control Attacks. URL: https://www.fortinet.com/resources/cyberglossary/command-and-control-attacks#:~:text=A%20Command%20and%20Control%20attack,the%20compromised%20network%20or%20machine.

8. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

9. Zillya. Руткіт – експерт з маскування шкідливого ПЗ. URL: https://zillya.ua/rutkit-ekspert-z-maskuvannya-shkidlivogo-pz.

10. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

11. Kraven Security. Cyber Kill Chain. URL: https://kravensecurity.com/cyber-kill-chain/.

12. Koroliuk, R., Nykytyuk, V., Tymoshchuk, V., Soyka, V., & Tymoshchuk, D. (2024). Automated monitoring of bee colony movement in the hive during winter season. CEUR Workshop Proceedings 3842, 184-195.

13. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

14. Dell. Сторінка підтримки Dell. URL: https://www.dell.com/support/kbdoc/ru-ua/000137973/.

15. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

16. ScienceDirect. Securing IoT Devices and Networks: Analysis and Recommendations. URL: https://www.sciencedirect.com/science/article/pii/S2542660523000306#sec6.

17. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081

18. NHS Digital. Cyber Alert 2017/CC-1513. URL: https://digital.nhs.uk/cyber-alerts/2017/cc-1513.

19. Fortinet. Command and Control Attacks. URL: https://www.fortinet.com/resources/cyberglossary/command-and-control-

attacks#:~:text=A%20Command%20and%20Control%20attack,the%20compromised%20network%20or%20machine.

20. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

21. Kraven Security. Cyber Kill Chain. URL: https://kravensecurity.com/cyber-kill-chain/.

22. European Union Publications. Baseline Security Recommendations for IoT. URL: https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a506-01aa75ed71a1/language-en.

23. Stanko, A., Wieczorek, W., Mykytyshyn, A., Holotenko, O., & Lechachenko, T. (2024). Realtime air quality management: Integrating IoT and Fog computing for effective urban monitoring. CITI, 2024, 2nd.

24. FreeCodeCamp. What is Nmap and How to Use It? A Tutorial for the Greatest Scanning Tool of All Time. URL: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/.

25. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

26. Medium. RouterSploit: Unleashing the Power of Router Penetration Testing. URL: https://medium.com/@S3Curiosity/routersploit-unleashing-the-power-of-router-penetration-testing-782f56b26004.

27. Stadnyk, M. (2016, February). The informative parameters determination for a visual system diagnostics by using the steady state visual evoked potentials. In 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET) (pp. 800-803). IEEE.

28. GeeksforGeeks. What is Burp Suite? URL: https://www.geeksforgeeks.org/what-is-burp-suite/.

29. Angryip. Angry IP Scanner. URL: https://angryip.org/

30. ASecurity. Angry IP vs Nmap. URL: https://7asecurity.com/blog/2011/04/angry-ip-vs-nmap/

31. Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. (2023). Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. In *ITTAP* (pp. 416-424).

32. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni, E., Peliukh, O., ... & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. *Information*, *14*(5), 259.

33. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. *Challenges to national defence in contemporary geopolitical situation*, *2022*(1), 55-61.

34. Ревнюк, О. А., Загородна, Н. В., Козак, Р. О., Карпінський, М. П., & Флуд, Л. О. (2024). The improvement of web-application SDL process to prevent Insecure Design vulnerabilities. *Прикладні аспекти інформаційних технологій*, *7*(2), 162-174.

35. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. In *Journal of Physics: Conference Series* (Vol. 1840, No. 1, p. 012026). IOP Publishing.

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ

2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професор.
Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.
Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.
Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.
Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com
Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.056.55

Тарас Микитюк[1]
[1]Тернопільський національний технічний університет імені Івана Пулюя, Україна

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ІОТ ПРИСТРОЇВ

Taras Mykytiuk

Penetration Testing of IoT Devices

З кожним днем Інтернет речей все більше інтегрується у повсякденне життя. Перевагами які надають IoT пристрої користуються не лише різного розміру бізнес а я звичайні люди які використовують IoT для різних повсякденних задач. Разом з всіма перевагами які пропонує IoT, користувачі ризикують отримати низку ризиків пов'язаних з вразливостями IoT систем як-от слабкі паролі, відсутність шифрування чи відсутність оновлень. Гучні інциденти зі залученням IoT зайвий раз підкреслюють небезпеку цих вразливостей і гостру необхідність їхнього своєчасного виявлення і оперативного виправлення. З боку розробників, вони повинні зробити все щоб кінцевий продукт був максимально захищеним, з боку користувачів, вони повинні забезпечити систематичне тестування на проникнення IoT-пристроїв щоб запобігти використання вразливостей зловмисником.

Дослідження спрямоване на аналіз реальних випадків атак на IoT-пристрої з метою визначення основних причин їх успіху та методів ідентифікації вразливостей. Зокрема, було проаналізовано такі інциденти:

- DDoS-атаки з використанням IoT-пристроїв, спричинені слабкими паролями;
- Компрометація IP-камер через незахищені веб-інтерфейси.

Методи аналізу включали розгляд відкритих джерел даних, стандартів OWASP IoT Top 10 та рекомендацій ENISA. Для кожного інциденту було запропоновано підходи, які дозволили б виявити вразливості під час тестування на проникнення. Наприклад:

- Для атак ботнету Mirai доцільним є використання сканерів паролів та автоматизованих засобів для виявлення відкритих портів;
- Для компрометації камер — аналіз мережевих конфігурацій і прошивок.

Результати дослідження демонструють, що інтеграція стандартів OWASP і ENISA дозволяє створити системний підхід до безпеки IoT. Запропоновані методики можна адаптувати до різних середовищ: від домашніх мереж до критичної інфраструктури. Практичні рекомендації включають посилення шифрування, регулярне оновлення прошивок та ізоляцію IoT-пристроїв у сегментованих мережах.

Дослідження показує, як використання сучасних інструментів тестування та аналізу може допомогти вчасно ідентифікувати ризики, зменшуючи ймовірність майбутніх інцидентів.

Література

1. Integrity360. "What is IoT Penetration Testing and Why Do You Need It?". URL: https://insights.integrity360.com/what-is-iot-penetration-testing-and-why-do-you-need-it. (дата перегляду 04.12.2024).
2. OWASP. "OWASP Internet of Things Project". URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10. (дата перегляду 04.12.2024).