УДК 004.056.55
Т. Микитюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ІОТ ПРИСТРОЇВ

UDC 004.056.55
T. 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).