Козарєзова О. А., здобувач
Галюс В.Ю., здобувач
Харченко С.А., здобувач
Петляк Н.С., асистент
Хмельницький національний університет

МОДЕЛЬ ВИЯВЛЕННЯ АТАК В IOT ЗА ДОПОМОГОЮ HONEYPOTS

З розвитком технологій Інтернету речей (IoT) відбулося стрімке зростання кількості підключених пристроїв, що використовуються в різних сферах: розумні будинки, промислові системи, медицина, транспорт та міська інфраструктура. Однак, широке впровадження IoT супроводжується значними викликами у сфері кібербезпеки, зокрема проблемою виявлення атак та аномалій. Однією із загроз є вразливість IoT-пристроїв через їхню обмежену обчислювальну потужність, відсутність вбудованих засобів захисту та використання застарілих або слабких протоколів аутентифікації. Адже багато виробників зосереджені на функціональності та доступності пристроїв, не приділяючи достатньої уваги їхній безпеці. IoT залишається вразливою ціллю для атак, що можуть включати несанкціонований доступ, інтеграцію шкідливих програм, експлуатацію вразливостей та використання IoT-інфраструктури для глобальних DDoS-атак. Таким чином, проблема виявлення атак та аномалій у IoT є складною і багатогранною. Вона вимагає розробки ефективних методів моніторингу, аналізу та реагування на загрози з урахуванням обмежених ресурсів IoT-пристроїв, різнорідності мереж та динамічної природи атак [1-2].

У роботі представлено ефективну модель виявлення атак у середовищі IoT, яка використовує технологію honeypots і складається з трьох основних взаємопов'язаних модулів.

Перший модуль відтворює реальну інфраструктуру IoT, створюючи обманний контур, що приваблює зловмисників і змушує їх взаємодіяти із системою. У ньому реалізовано емуляцію IoT-пристроїв, що генерують реалістичний мережевий трафік та взаємодіють за допомогою протоколу MQTT. Це змушує зловмисників сприймати систему як справжню мережеву інфраструктуру з критично важливими даними та потенційними слабкими місцями. Окрім емуляції пристроїв, у цьому модулі розгорнуто Honeypot, який працює у середовищі Python Virtual Environment та приймає вхідні з'єднання через стандартні для IoT-систем порти, зокрема SSH і Telnet. Він записує всі взаємодії зловмисників, включаючи введені команди, спроби завантаження шкідливого програмного забезпечення та інші дії, що можуть свідчити про атаку.

Другий модуль, хостове середовище, забезпечує обчислювальні ресурси для функціонування симульованого середовища та Honeypots. Воно складається з двох віртуальних машин: Windows та Linux. Перша віртуальна машина виконує роль симулятора IoT-пристроїв, використовуючи BevyWise IoT Simulator, що забезпечує реалістичне функціонування мережі та обмін даними між компонентами. Також на ній розгорнуто веб-інтерфейс для візуалізації активності IoT-пристроїв у режимі реального часу. Друга машина використовується як серверна платформа для розміщення Honeypot-системи, яка реєструє спроби несанкціонованого доступу та аналізує вхідні з'єднання. Всі елементи цього середовища працюють у межах сегментованої VLAN-мережі, що дозволяє відокремити тестове середовище від реальних інфраструктурних ресурсів та забезпечити безпеку експерименту.

Третій модуль, поверхневе середовище, відповідає за збір, збереження та аналіз отриманих даних. Всі журнали активності, що фіксують спроби атак, передаються у спеціалізовані системи логування, де вони проходять подальший аналіз. Застосування Splunk дає можливість аналізувати отримані журнали, систематизувати інформацію про атаки та будувати візуальні моделі поведінки зловмисників. У логах зберігається інформація про IP-адреси, методи злому, введені команди та можливі вектори атак.

Запропонована модель демонструє високу достовірність та ефективність у виявленні загроз у середовищах Інтернету речей. На відміну від класичних підходів до кібербезпеки, ця модель дозволяє не просто виявляти загрози в реальному часі, а й досліджувати динаміку атак, що дає змогу покращувати стратегії захисту. Гнучка архітектура та можливість розширення роблять цю модель універсальним рішенням для захисту IoT-систем різного рівня складності.

Список використаних джерел:

1. Khan A. R., Kashif M., R. H. Jhaveri, Roshani R., Tanzila S., Bahaj S. A. Deep learning for intrusion detection and security of internet of things (IoT): current analysis, challenges, and possible solutions. *Security and Communication Networks*. 2022. DOI: 10.1155/2022/4016073

2. Taherdoost H. Security and Internet of Things: benefits, challenges, and future perspectives. *Electronics*. 2023. Vol. 12, No 8. DOI: 10.3390/electronics12081901