УДК 004.7, 004.62

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖІ IOT

Гіззатуллін Д. Д., Курдеча В.В.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: deny.gizz@gmail.com

THE METHOD FOR DETECTING INTRUSIONS INTO AN IOT NETWORKS

Modern network intrusion detection methods are analyzed. Considered the advantages and disadvantages of using a neural network method of intrusion detection. Prospects for the use of neural network methods are considered. Proposed scheme of intrusion detection system based on a neural network.

Проаналізовано сучасні методи виявлення вторгнень у мережу. Розглянуто переваги та недоліки використання нейромережевого методу виявлення вторгнень. Розглянуто перспективи використання нейромережевих методів. Запропоновано метод виявлення вторгнень на основі нейронної мережі.

По даним експертів [1] та аналітиків [2] кількість атак на мережі IoT зростає. За першу половину 2019 року серверам-пасткам, які видають себе за IoT пристрої, вдалось зафіксувати 105 млн атак на пристрої IoT, що приблизно в 9 разів більше ніж за аналогічний період 2018 року, де було зафіксовано 12 млн атак. Розвиток IoT нерозривно пов'язаний з ростом потенційно вразливих пристроїв. Користуючись слабким захистом IoT-продуктів, кіберзлочинці прикладають все більше зусиль для створення і монетизації IoT-ботнетів.

Одним із кроків направлених на підвищення безпеки, являється використання систем виявлення вторгнень. Дані системи спрямовані виявлення аномалій в мережевому трафіку, що являють собою небажаний зловмисний трафік.

В наш час системи виявлення вторгнень базується переважно на поєднанні сигнатурних та статистичних методів.

Сигнатурні методи дозволяють описати атаку на мережу певним набором правил, або за допомогою формальної моделі, яка наприклад може представляти собою семантичний вираз на спеціальній мові.

Суть даного методу полягає у використанні спеціалізованої бази шаблонів (сигнатур) атак для пошуку дій, що підпадають під визначення “атака”. Такий метод може захистити від атак, сигнатури яких уже присутні в базі даних

системи виявлення вторгнень. У виявленні аномалій значну роль відіграє вибір оптимальної кількості врахованих параметрів оцінки, а також визначення загального показника стану аномальності в захищеній системі [3].

Основним недоліком сигнатурних методів являється здатність системи виявити атаки невідомих типів. БД експертної системи повинна містити сценарії більшості відомих на сьогоднішній день атак.

Для того щоб усунути недоліки таких систем доцільно застосовувати клас методів виявлення вторгнень, який повністю покладається на статистичний апарат.

Статистичні методи основані на припущені, що для певної системи існує свій профіль нормального стану і будь-які значні відхилення від цього стану являється ймовірним кандидатом на можливу атаку. Для побудови базового нормального профілю системи використовується статистичний набір даних, вільному від аномалій.

На відміну від сигнатурних методів, статистичні можуть виявляти нові типи мережевих атак, для яких ще не існує певної сигнатури. Системи виявлення вторгнень основані на статистичних методах не потребують оновлення сигнатурних БД, що значно спрощує експлуатацію системи.

Серед недоліків таких систем виявлення вторгнень можна відмітити складність завдання порогових значень, що являє собою не тривіальну задачу, яка потребує глибоких знань про підконтрольну систему. Статистичні методи нечутливі до порядку слідування подій[3].

Одним із варіантів усунення недоліків попередніх систем, може бути використання нейромережевих методів виявлення вторгнень. Всі методи виявлення вторгнень базуються на визначенні певного набору параметрів співставлення яких з параметрами функціонування мережі в певний момент часу дає змогу судити про наявність втручання в роботу мережі. Беручи до уваги здатність нейромереж оптимізувати свої параметри в ході свого навчання, можна вважати дослідження нейромережевих методів вельми перспективними.

На відміну від сигнатурних методів, нейромережі можуть самі визначати важливість певних параметрів, значення яких впливають на рішення про вторгнення в мережу, так як нейромережа, в ході свого навчання, встановлює закономірності в атаках[3]. В той самий час мережа сама признаки нормального функціонування мережі, і визначає порогові значення, відхилення від яких є небажаними в мережі.

Рис. 1. Приклад схеми архітектури нейромережевої системи виявлення вторгнень.

На рис.1 запропоновано схему системи виявлення вторгнень на базі нейромережі.

Головною перевагою нейромережевих методів є можливість навчання з ціллю створення гнучких адаптивних систем. Також перевагою є можливість використання уже навчених ядер нейромереж, з наступним перенавчанням під власні цілі. Також на відміну від статистичних методів, деякі архітектури нейромереж здатні аналізувати часові послідовності.

Література

1. SECURELIST [Електронний ресурс] / Ден Деметр, Марко Пройсс, Ярослав Шмелев. Отчёт безопасности устройств за 2019 год — Режим доступа: https://securelist.ru/iot-a-malware-story/94900/ (дата публикации: 19.12.2019).
2. Posetive Technologes [Електронний ресурс] / Актуальные киберугрозы. II квартал 2018 года — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2/ (дата публикации: 13.09.2018).
3. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2013. – 220 с.
4. M. Roopak, G. Yun Tian and J. Chambers, "Deep learning models for cyber security in IoT networks", pp. 0452-0457, 01 2019.