УДК 004.45

Н. М. Ковтун; Р. О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ЗАСОБІВ ПРОТИДІЇ ВТОРГНЕННЯМ І АТАКАМ НА КОМП'ЮТЕРНІ СИСТЕМИ

N. M. Kovtun; R.O. Zharovskyi, Ph.D.

ANALYSIS OF MEANS OF RESISTING INTRUSIONS AND ATTACKS ON COMPUTER SYSTEMS

У питанні захисту інформації в комп'ютерних системах дуже велике значення для запобігання несанкціонованому доступу мають системи виявлення та запобігання атакам.

Такі системи в реальному часі відстежують аномальну активність на підставі потоків даних, що одержуються з інформаційних систем, мережевого обладнання, антивірусних додатків, систем запобігання витоку даних та багатьох інших джерел. Системи виявлення вторгнень можуть моніторити весь трафік мережі, що дозволяє їм виявляти підозрілі активності, навіть якщо вона відбувається всередині захищеної мережі.

Однак, способи та методики мережевих вторгнень постійно змінюються та модернізуються зловмисниками. У таких динамічних умовах необхідний перегляд алгоритмів, що використовуються в роботі СВВ (системи виявлення вторгнень), для надійної роботи системи. Нові алгоритми роботи повинні спиратися не тільки на сигнатури відомих інструментів та методів, але й адаптуватись до нових загроз.

Для вирішення завдання щодо вдосконалення систем виявлення та запобігання атак дослідники виділяють кілька основних напрямків:

- вдосконалення сигнатурного та статистичного аналізу даних;
- обробка нечітких онтологій на підставі попередньо затвердженої безпекової політики;
- використання нейромереж для постійного навчання IDS-системи та протидії складнопрогнозованим атакам.

Принцип роботи IDS-систем заснований на аналізі мережної чи системної активності та пошуку відхилень від нормальної поведінки. Для цього IDS використовують моделі поведінки, які можуть бути створені на основі статистичних даних про те, як повинен проходити обмін даними всередині системи.

IDS можуть працювати в режимі реального часу, постійно переглядаючи та аналізуючи дані, або виконуватись за розкладом, скануючи систему у певні моменти часу.

Як правило IDS поєднують у собі як сигнатурні методи, так і поведінковий аналіз, що збільшує загальний рівень безпеки системи, але також підвищується кількість помилкових спрацьовувань. Також система може включати в себе модуль прийняття рішень та модуль реагування, що забезпечує можливість реагувати на вторгнення та запобігати атакам. Загальна схема архітектури IDS зазначена на рисунку 1.

Функціональність модуля виявлення атак спрямована на аналіз стану мережі та реєстрацію подій підозрілої активності або комп'ютерних атак. Модуль прийняття рішень отримує дані щодо здійснених атак від модуля виявлення атак і, базуючись на різних параметрах, відправляє відповідні команди модулю реагування [1]. Реакції на атаку можуть включати блокування конкретної IP- або MAC-адреси пристрою, встановлення тимчасових або постійних правил для міжмережевих екранів мережевого

обладнання, а також блокування або позбавлення привілеїв облікових записів систем, включаючи доменні. Інші можливі дії включають інформування оператора IDS або системного адміністратора тощо.

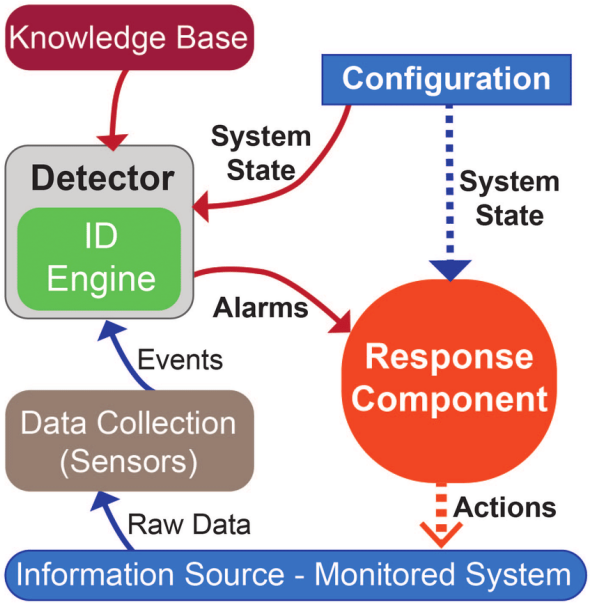

Рисунок 1. Архітектура IDS

Атаки на мережевому, прикладному та канальному рівнях проходять через фільтрацію бази знань. Мережевий трафік піддається контролю підсистемою сенсорів, які в реальному часі фільтрують пакети за заздалегідь визначеними правилами, характерними для найпоширеніших атак. Сенсори копіюють пакети і передають їх модулю виявлення атак та сховищу. Сенсори використовують сигнатурний метод аналізу трафіку, отримуючи інформацію про шаблони проведення атак із бази знань [2].

База знань також включає шаблони реагування на інциденти, які сприяють модулю прийняття рішень у виборі найбільш підходящого способу реагування. Модулі IDS керуються оператором через консоль управління, що дозволяє IDS взаємодіяти та діагностувати стан мережі та інформаційних систем всередині неї.

Сучасні дослідники також розглядають можливість використання технологій нейронних мереж та інтелектуального аналізу даних для роботи IDS-систем [3, 4,] Згідно з вищезазначеним дослідженням, найбільш оптимальним з точки зору безпеки є комбінація кількох алгоритмів виявлення атак за участю програмного арбітра, який визначає рівень моделі OSI та тип мережної активності для вибору подальшого алгоритму аналізу трафіку

Література

1 Deconstructing the Computer: Report of a Symposium / Committee on Deconstructing the Computer, Committee on Measuring and Sustaining the New Economy, Board on Science, Technology, and Economic Policy, Policy and Global Affairs, National Research Council - Washington: National Academies Press, 2005. - P. 49-50.

2 Adaptation Techniques for Intrusion Detection and Intrusion Response Systems URL: http://www.secdev.org/idsbiblio/adapt.pdf

3. Batista, L. O., de Silva, G. A., Araujo, V. S., Araujo, V. J. S., Rezende, T. S., Guimarães, A. J., Souza, P. V. D. C. Fuzzy neural networks to create an expert system for detecting attacks by sql injection. 2019 . URL: https://arxiv.org/abs/1901.02868

4. Mahdavifar, S., Ghorbani, A. A. DeNNeS: deep embedded neural network expert system for detecting cyber attacks. Neural Computing and Applications. 2020. URL: https://link.springer.com/article/10.1007/s00521-020-04830-w