УДК 004.45
Н.М. Ковтун; Р.О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

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

ALGORITHMIC PROVISION OF INTRUSION DETECTION SYSTEMS

На підставі аналізу літератури, наукових та аналітичних статей з проблеми вдосконалення систем виявлення вторгнень та попередження комп'ютерних атак було виділено критерії оцінки інформації, що захищається, визначено основні інструменти її захисту, а також сформульовано завдання, яке вирішують системи виявлення вторгнень.

У ході роботи було проведено класифікацію IDS/IPS-систем, виявлено способи їх розміщення, алгоритми роботи та методи отримання даних. Визначено сильні та слабкі сторони кожного згаданого класу.

Були проаналізовані алгоритми, які у роботі системи виявлення вторгнень, як із використанням класичних сигнатурних алгоритмів, і більш сучасних методів поведінкового аналізу та інтелектуального аналізу даних. Також було визначено схему архітектури системи виявлення вторгнень.

За результатами аналізу було зроблено висновок необхідність застосування системи виявлення вторгнень комбінації алгоритмів аналізу трафіку щодо різних рівнів мережевої моделі OSI і типів мережевої активності.

Розглянемо докладніше існуючі алгоритми, які у системах виявлення вторгнень. IDS виявляють атаки шляхом використання різних методів аналізу вихідних даних. У цій дослідницькій роботі торкнемося наступні методи виявлення атак:

– packet header anomaly detection (PHAD) – аналіз заголовків пакетів трафіку;
– network traffic anomaly detection (NETAD) – аналіз вмісту кадрів мережного трафіку;
– application layer anomaly detection (ALAD) – аналіз роботи додатків;
– learning rules for anomaly detection (LERAD) – умовні правила виявлення аномалій у вихідних даних пакетів (наприклад, ланцюжки handshake, що передаються в рамках TCP-сесії).

Кожен метод виявлення атак показує найбільшу ефективність проти певних видів атак. Наприклад, аналіз заголовків ефективний виявлення атак типу DNS-spoofing чи SYN-flood, але з здатний виявити використання SQL-ін'єкцій, яке, своєю чергою, легко виявляється з допомогою аналізу роботи додатків.

Тому в більшості систем виявлення вторгнень використовуються комбінації різних методів виявлення атак разом з попередньо налаштованими правилами та/або технологіями машинного навчання для забезпечення найбільшої безпеки системи, що захищається, і мінімізації можливої шкоди.

Незважаючи на те, що методи виявлення аномалій удосконалюються з кожним роком, першим етапом роботи будь-якого IDS є сигнатурний аналіз. Він дозволяє максимально швидко виявити найпоширеніші атаки без залучення основних ресурсів системи, що економить час та обчислювальні потужності серверів.

Ефективність роботи алгоритмів визначається наступним рядом параметрів: швидкість обчислень (час обробки вихідних даних), точність визначення атак (достовірність визначення факту атаки та її правильна класифікація), частота помилкових спрацьовувань системи.