Дослідження відкритих сигнатурних систем виявлення аномалій

Владислав Труш, Андрій Сторожов, Олександр Федюшин

Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: vladyslav.trush@nure.ua, andrii.storozhov@nure.ua , oleksandr.fediushyn@nure.ua

***Коротка анотація** – A comparative analysis of the characteristics of modern open source anomaly detection systems was performed. The comparison this system was performed on the following indicators: monitoring level, response type, adaptive capacity, architecture, detection method supported for platform deployment, principle of construction, method of extending functionality.*

Ключові слова – системи виявлення аномалій, сигнатури, мережні атаки, Snort, Suricata, Bro, OSSEC, Prelude.

I. Вступ

В епоху цифрових технологій однієї із ключових проблем у сучасному суспільстві є захист інформації. Це приводить до створення певних систем і засобів, які повинні мати у своїй наявності на мережному рівні деякі механізми захисту й протидії хакерським загрозам. У цей час вважається важливим забезпечити найбільший рівень захищеності в корпоративних мережах будь-якої організації, яка зберігає критично важливі дані. Успіх і конкурентоспроможність такої організації багато в чому залежать саме від використання ефективних засобів, що задовольняють умовам вище.

Одним з найбільш відомих засобів, що добре зарекомендували себе, для розв'язання цього завдання є системи виявлення аномалій (СВА) [1]. По способу збору інформації виділяють хостові та мережні СВА. У даній роботі акцент зроблений убік дослідження та критичного аналізу тих СВА, які функціонують саме на мережному рівні. Такі СВА можна визначити як програмні або апаратні пристрої, призначені для виявлення спроб несанкціонованого доступу, фактів порушення безпеки в рамках мережної взаємодії між хостами та будь-яких інших аномальних дій у комп'ютерній мережі.

II. Аналіз проблеми

Для виявлення мережних атак можуть застосовуватися як сигнатурні механізми пошуку шаблонових аномальних дій, так і евристичні (статистичні, нейромережні, імунні та ін.) підходи. У випадку сигнатур [1-4] розв'язання завдання зводиться до реалізації процедури, що виконує перевірку входження заданої байтової послідовності усередині вмісту мережних пакетів. Недоліками такого розв'язку є складність створення репрезентативного набору з подібними записами й обмеження у виявленні модифікованих варіантів відомої атаки. Навпаки, евристичні підходи дозволяють виявляти сховані закономірності в аналізованих мережних потоках. Саме ця особливість пояснює їхню широку популярність у науково-дослідницькому співтоваристві й відіграє ключову роль при виборі й проектуванні ядра СВА. З іншого боку, в основі функціонування більшості комерційних і відкритих програмних рішень переважає підхід, який базується на сигнатурному зіставленні зі зразком і характеризується мінімальним числом неправильних спрацьовувань. Для збереження переваг обох підходів використовується прийом їх комбінування, який як і раніше залишається не повною мірою дослідженим. Тому завдання виявлення аномальних мережних з'єднань є актуальним.

III. Розв'язання проблеми

Для огляду були обрані п'ять СВА, які мають відкритий програмний код і поширюються по безкоштовних ліцензіях GNU GPL і BSD. Серед них представлені Snort, Suricata, Bro, OSSEC, Prelude [2,4]. Аналіз даних СВА проводився на рівні вивчення їх вихідних текстів, керівництв користувача, програмної документації й інших джерел технічної та наукової літератури, що перебувають у відкритому доступі.

У Табл. 1 представлені порівняльні характеристики і їх значення для кожної із представлених вище СВА.

Порівняння СВА проводилося за наступними показниками: рівень моніторингу, тип реагування, адаптивна здатність, архітектура, метод виявлення, підтримувані для розгортання платформи, принцип побудови, спосіб розширення функціональності.

Майже всі описані СВА є активними. Виключенням із цього списку є лише Bro, яка не має вбудованих засобів для запобігання атак, однак за допомогою модуля, що йде в поставці з нею, exec.bro можна настроїти примусове скидання підозрілого з'єднання або блокування трафіка на рівні ядра за допомогою правил IPtables. Це анітрошки не збіднює дану платформу, оскільки згідно із джерелом [1] Bro розроблялася в першу чергу саме для вивчення характеристик мережного трафіка, а не для виявлення в ньому атак. Із цією метою в ній були реалізовані потужні аналізатори протоколів, що дозволили ідентифікувати тип протоколу навіть на нестандартних портах завдяки механізму DPD (Data Packet Detection, Dynamic Protocol Detection), який аналогічний застосовуваному в Suricata. Крім того, при розробці Bro позначилося її минуле: вона розвивалася в академічному оточенні, тому характеризується властивістю адаптивності за рахунок наявності в її основі статистичних модулів виявлення мережних аномалій: спроб сканування портів (scan.bro), проведення Dos-атак (synflood.bro). Усі із представлених СВА є кроссплатформеними, за винятком Bro, яка призначена для запуску тільки в Unix-подібних ОС. Також відзначимо, що для

ТАБЛИЦЯ 1.

ПОРІВНЯЛЬНІ ХАРАКТЕРИСТИКИ СВА

Хар-ка	Snort	Suricata	Bro	Prelude	OSSEC
Рівень моніторингу	Мережний	Мережний	Мережний	Мережний та хостовий	Хостовий
Тип реагування	Активний	Активний	Пасивний	Активний	Активний
Здатність до адаптації	Додатковий модуль	Додатковий модуль	Статистичний аналіз	Відсутній	Відсутній
Архітектура	Централізована	Централізована	Централізована	Розподілена	Розподілена
Платформи	Windows, *nix	Windows, *nix	*nix	Windows, *nix	Windows, *nix
Спосіб розширення	Динамічно завантажувані декодери	Динамічно завантажувані so/dll бібліотеки, Lua-скрипти	Bro-сценарії, so-бібліотеки	Сенсори, що підключаються	XML-правила

платформи Windows система OSSEC не має режиму локальної установки, тобто для цієї ОС необхідно встановлювати окремо й сервер, і агенти. І в той же час саме OSSEC є єдиною із представлених СВА, здатною виявляти шкідливі процеси як наслідки успішно реалізованих атак. Для систем Snort і Suricata властивість адаптивності найчастіше реалізується через додаткові модулі. Зустрічаються як вітчизняні, так і закордонні дослідження, у яких автори вбудовують в Snort такі інтелектуальні декодери, приміром, на основі нейронних мереж, методу опорних векторів і дерев розв'язків. За принципом побудови можна класифікувати дані системи як монолітні та компонентні. У першому випадку система представлена як єдиний бінарний файл, запуск якого засобами ОС, як правило, породжує не більш одного процесу. До них з розглянутих СВА належать Snort, Suricata і Bro. Компонентний підхід має на увазі розбивку системи на кілька функціональних блоків, кожний з яких запускається в окремому просторі пулу адрес пам'яті, виконує конкретне завдання й спілкується з іншими на основі механізмів міжпроцесної взаємодії. До ряду таких систем належать OSSEC і Prelude. Як уже було відзначено раніше, основними елементами для створення додаткових функцій у роботі систем Snort і Suricata є декодери й препроцесори, основа функціонування яких полягає у виклику певних функцій з динамічно завантажуваних бібліотек (so/dll). Найбільш просунутий спосіб створення нових модулів, що розширюють функціональні можливості системи, має Bro. Уся рутинна робота з написання шаблонових файлів майбутнього додатка зведена до мінімуму. Разом з вихідними кодами даної системи поставляється bash-скрипт init-plugin, призначений для автоматичної генерації початкового кістяка майбутнього модуля, правил його складання й установки. Після компіляції модуль являє собою готову so-бібліотеку, прототипи функцій з якої обгорнені у відповідний bro-скрипт. Наступне завантаження, ініціалізація покажчиків на функції та деалокація модулів системою зводяться до виклику функцій dlopen, dlsym і dlclose відповідно.

Висновки

В роботі проведений порівняльний аналіз характеристик сучасних відкритих систем виявлення аномалій.

Серед розглянутих СВА найбільш повні характеристики має Prelude. Будучи спроектованою з самого початку розподіленою системою, вона підтримує гібридний моніторинг контрольованих вузлів, здійснюючи аналіз як на рівні мережі, так і на рівні хоста. Крім того, ця система є масштабованою, що дозволяє їй використовувати безліч різнорідних джерел для збору й обробки даних. Модульний принцип установки цієї системи також дозволяє добитися більш гнучкого настроювання кожного з її компонентів окремо. Можливість підключення кожної із представлених СВА в якості сенсорів для Prelude (для Bro необхідно реалізовувати нового клієнта вручну, тому що для неї немає готового сенсора) ставить її на ранг вище інших СВА.

Література

[1] Rødfoss, J. T. Comparison of open source network intrusion detection systems / J. T. Rødfoss: MA thesis / Rødfoss, Jonas Taftø. — University of Oslo, Department of Informatics, 2011. — 85 pp.

[2] Sanders, C. Applied network security monitoring: collection, detection, and analysis / C. Sanders, J. Smith. — Elsevier, 2013. — 496 pp.

[3] ntop. Accelerating Snort, Bro and Suricata with PF RING ZC [Електронний ресурс]. – URL: http://www.ntop.org/pf ring/acceleratingsnort-bro-and-suricata-with-pf ring-zc/

[4] Zaraska, K. Prelude IDS: current state and development perspectives / K. Zaraska [Електронний ресурс]. – 2003. – URL: http://citeseerx.ist.psu.du/viewdoc/download?doi=10.1.1.106.5542%5C&rep=rep1%5C&type=pdf.