Порівняльний аналіз систем виявлення і запобігання вторгнень

Олександр Риков[1], Інна Олешко[1]

1. Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
УКРАЇНА, м. Харків, пр. Науки, 14,
E-mail: oleksandr.rykov@nure.ua

Коротка анотація – The article is written about multitasking protecting program that helps users detecting intruders. It deals with application and shows how people can use this app to prevent stealing of their data. It was shown, that the Suricata program is one of the most popular and fast protector.

Ключові слова - адміністратор, трафік, мережева атака, Suricata, IDS, IPS, Snort.

I. Вступ

У сучасному світі системи виявлення та запобігання вторгнень (Intrusion detection system / Intrusion prevention system, IDS / IPS) - необхідний елемент захисту від мережевих атак. Основне завдання даних систем - виявлення фактів несанкціонованого доступу в корпоративну мережу або несанкціонованого управління нею, з виконанням відповідних заходів протидії (інформування адміністраторів про факт вторгнення, обрив з'єднання або перенастроювання брандмауера для блокування подальших дій зловмисника і т.д.).

Існує багато систем виявлення та запобігання вторгнень. Актуальною є задача вибору однієї з них. У роботі проводиться порівняльний аналіз систем виявлення вторгнень, робиться висновок про те, що система Suricata є більш швидким та надійним детектором атак.

II. IDS / IPS-рішення

IDS / IPS системи - це унікальні інструменти, створені для захисту мереж від несанкціонованого доступу. Вони являють собою апаратні або комп'ютерні засоби, які здатні оперативно виявляти і ефективно запобігати вторгненням. Серед заходів, які приймаються для досягнення ключових цілей IDS / IPS, можна виділити інформування фахівців з інформаційної безпеки про факти спроб хакерських атак і впровадження шкідливих програм, обрив з'єднання зі зловмисниками і перенастроювання мережевого екрану для блокування доступу до корпоративних даних.

Кібератаки - одна з основних проблем, з якими стикаються суб'єкти, які мають інформаційними ресурсами. Відомі антивірусні програми і брандмауери ефективні лише для захисту очевидних місць доступу до мереж. Однак зловмисники здатні знаходити шляхи обходу і вразливі сервіси навіть в найдосконаліших системах безпеки. При такій небезпеці не дивно, що закордонні та українські UTM-рішення отримують все ширшу популярність серед організацій, що бажають виключити можливість вторгнення і поширення шкідливого ПЗ (хробаків, троянів і комп'ютерних вірусів). Багато компаній приймають рішення купити сертифікований міжмережевий екран або інший інструмент для комплексного захисту інформації.

Всі існуючі сьогодні системи виявлення та запобігання вторгнень об'єднані кількома загальними властивостями, функціями і завданнями, які з їх допомогою вирішують фахівці з інформаційної безпеки. Такі інструменти за фактом здійснюють безперервний аналіз експлуатації певних ресурсів і виявляють будь-які ознаки нетипових подій.

Організація безпеки корпоративних мереж може ґрунтуватися на кількох технологіях, які відрізняються типами виявлених інцидентів і методами. Крім функцій постійного моніторингу та аналізу того, що відбувається, IDS системи виконують такі функції:

- збір і запис інформації;
- оповіщення адміністраторів мереж про зміни, що відбулися;
- створення звітів для підсумовування логів.
- Технологія IPS в свою чергу у додачу до вище сказаного, здатна не тільки визначити загрозу і її джерело, а й здійснити їх блокування. Це говорить про розширений функціонал подібного рішення. Вона здатна здійснювати наступні дії:
- обривати шкідливі сесії і запобігати доступу до найважливіших ресурсів;
- змінювати конфігурацію «підзахисної» середовища;
- проводити дії над інструментами атаки (наприклад, видаляти заражені файли).

Варто відзначити, що UTM-міжмережевий екран і будь-які сучасні системи виявлення та запобігання вторгнень є оптимальною комбінацію технологій систем IDS і IPS.

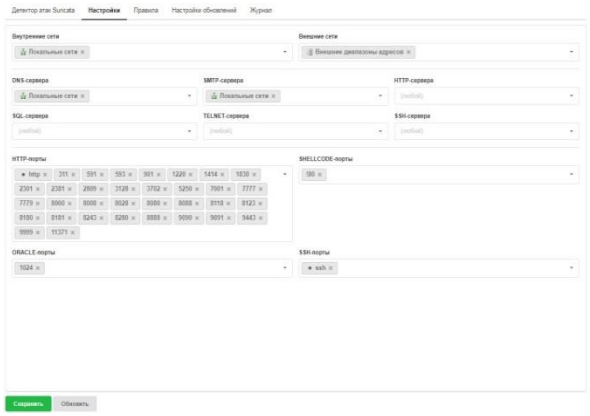
III. Детектори атак Suricata

Одним з рішень IPS запобігання вторгнень є детектори атак, які призначені для своєчасного виявлення безлічі шкідливих загроз. В Інтернет Контроль Сервері вони реалізовані у вигляді системи Suricata - багатозадачного і продуктивного інструменту, розробленого для захисту мереж, а також збору і зберігання інформації про будь-які сигнали, що надходять. Робота детектора атак заснована на аналізі сигнатур і евристиці, а зручність його обумовлено наявністю відкритого доступу до вихідного коду. Такий підхід дозволяє налаштовувати параметри роботи системи для вирішення індивідуальних завдань.

До редагованих параметрів Suricata відносяться правила, яким буде підпорядковуватися аналіз трафіку, фільтри, що обмежують висновок попередження адміністратора, діапазони адрес різних серверів, активні порти і мережі.

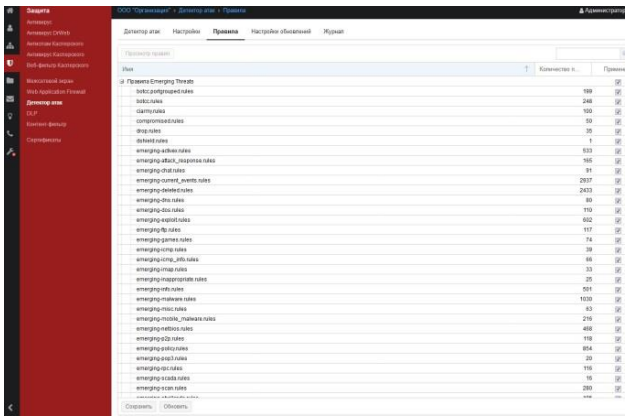
Таким чином, Suricata, як IPS-рішення - це досить гнучкий інструмент, функціонування якого підлягає змінам в залежності від характеру атаки, що робить його максимально ефективним.

В ІКС фіксується і зберігається інформація про підозрілу активність, блокуються ботнети, DOS-атаки, а також TOR, анонімайзери, P2P і торрент-клієнти.



Малюнок 1 – Настройка “Suricata”

У вкладці налаштувань (малюнок 1) можна редагувати параметри роботи детектора атак. Тут можна вказати внутрішні, зовнішні мережі, діапазони адрес різних серверів, а також порти, що використовуються. Всім цим змінним присвоєно значення за замовчуванням, з якими детектор атак може коректно запуститися. За замовчуванням, аналізується трафік на зовнішні інтерфейси.



Малюнок 2 – Правила “Suricata”

Детектору атак можна підключати правила, за допомогою яких він буде аналізувати трафік. На вкладці на малюнку 2 можна подивитися наявність і вміст того чи іншого файлу з правилами, а також включити або виключити його дію (за допомогою прапорців праворуч). У правому верхньому куті розташовується пошук за назвою або за кількістю правил у файлі.

IV. Порівняння Suricata та Snort

Більше 250 одиничних тестів було проведено проти Suricata та Snort, дотримуючись методології, результати наведені в Таблиці 1.

ТАБЛИЦА 1

РЕЗУЛЬТАТИ ТЕСТІВ

Тестова група	Кількість тестів	Оцінка suricata	Оцінка snort
Поганий трафік	4	1	1
Роздроблені пакети	2	1	3
Шкідливі програми та віруси	14	9	7
Відмова в обслуговуванні (DoS)	3	3	3
Атаки з боку клієнта	257	157	127
Оболонки	12	12	7
Продуктивність	0	2	1
Всього	297	185	149

Випробування були проведені на 14 шкідливих програмах та вірусах. Suricata має кращий рівень виявлення шкідливих програм та вірусів, ніж Snort.

На наборі з 11 оболонок (вірус схований в іншому файлі), Suricata виявив 9 shellcodes, а Snort виявив 7 shellcodes.

У наборі з 3 тестів і Suricata, і Snort виявили 3 спроби DoS проти служб SSH та MSSQL.

Тести продемонстрували, що Suricata краща, ніж Snort для виявлення нападів на стороні клієнта, зі швидкістю виявлення 82% проти 49%.

Висновки

За результатами наведеного вище аналізу робимо висновок про те, що детектор атак Suricata – швидка та досить надійна систем, яка вміє по максимуму використовувати можливості сучасних процесорів і GPU. Мінус цієї системи - велика кількість налаштувань і недостатньо виразна в деяких питаннях документація. Проте, після установки, система досить добре працює з настройками за замовчуванням, а з тонким налаштуванням досвідчений адміністратор безпеки розбереться без проблем.

Література

[1] Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980.

[2] Електронний ресурс https://oisf.net (дата звернення 20.10.2019)

[3] Електронний ресурс https://suricata-ids.org (дата звернення 20.10.2019)