УДК 004.45
Касьян К.М.[1], Головіна К.П.[2]
[1] канд. техн. наук. НУ «Запорізька політехніка»
[2] студ. гр. КНТ-510м НУ «Запорізька політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Метою є виявлення поширених методів виявлення мережевих атак і вибір найбільш ефективного на даний момент рішення. У роботі наводиться методика порівняння ПЗ систем виявлення вторгнень, обґрунтування вибору характеристик для порівняння і результати проведення порівняння на основі отриманої методики. В результаті порівняльного аналізу виявилося кілька кращих продуктів: ПЗ з відкритим вихідним кодом Snort і розробка Фонду Відкритої Інформаційної Безпеки Suricata

Мережеві атаки - неминуча загроза будь-якого пристрою, підключеного до мережі Інтернет. В результаті успішної реалізації такої атаки можливий несанкціонований доступ до комп'ютера, вихід з ладу сервера, витік даних. безумовно, це одна з головних проблем інформаційної безпеки.

Для запобігання подібних атак актуальним завданням стає виявлення спроби здійснення мережевої атаки. Клас програм, що вирішують цю задачу, отримав назву «система виявлення вторгнень (СВВ)».

Система виявлення вторгнень - програмне (апаратне, програмно-апаратний) засіб, що виявляє факт несанкціонованого, несанкціонованого доступу до пристрою. Стандартна архітектура СВВ включає наступні підсистеми:

— Сенсорна підсистема. Складається з «датчиків», які збирають інформацію про абітурієнта трафіку і стан об'єкта, що захищається.

— Підсистема аналізу. Отримує дані від сенсорної підсистеми і виносить вердикт про факт спроби мережевої атаки.

— Місце. Накопичує дані про події інформаційної безпеки, отриманих від підсистеми аналізу.

— Панель управління. Програмний модуль, дозволяє конфігурувати СВВ, спостерігати поточний стан системи, переглядати інциденти безпеки. [1]

Система виявлення вторгнень має кілька можливих виконань:

— Мережева СВВ. Відстежує атаки, аналізуючи мережевий трафік і спостерігаючи за декількома хостами. Отримує доступ до трафіку, будучи підключена до хабу або світчу. Одним з найяскравіших прикладів мережевої СВВ є open-source ПЗ Snort.

— СВВ, заснована на протоколі Protocolbased IDS. Аналізує комунікаційні протоколи зв'язку. У разі виконання на веб-сервері в основному аналізує HTTP і HTTPS з'єднання. При аналізі HTTPS з'єднання СВВ повинна мати доступ до трафіку до його шифрування і відправлення.

— СВВ, заснована на прикладних протоколах Application Protocol-based IDS. Аналізує специфічні для певного додатка протоколи. У разі захисту SQL бази даних аналізу піддаються всі SQL запити.

— Вузлова СВВ (Host-based IDS). Будучи розташованої на хості, відстежує вторгнення, аналізуючи системні журнали подій, логи додатків, модифікації файлів. Найбільш популярним програмним рішенням даного виду СВВ OSSEC.

— Гібридна СВВ. Поєднує два і більше підходів до визначення атак. Є найбільш кращим варіантом з огляду на створення найбільш повного уявлення про безпеку комп'ютерної мережі. Прикладом гібридного виконання СВВ є ПЗ Prelude. [2]

З класифікації можна зробити висновок: основним моментом порівняння ПЗ є вид виконання СВВ. Однак метод визначення атак в СВВ ключовим моментом в порівнянні.

Основні класи методів визначення мережевих атак:

— Кореляційні. Методи, засновані на машинному навчанні. Характеризуються здатністю виявляти не закладені в базу аномалії, але також наявністю високого рівня помилкових спрацьовувань.

— Сигнатурні методи. Засновані на порівнянні поточного стану мережі з шаблонами, наявними в базі сигнатур. Характеризуються відсутністю помилкових спрацьовувань, але також вкрай низькою ймовірністю визначення аномалії, що не міститься в базі.

СВВ також має два подання з режиму роботи: пасивний і активний. Визначення мережевої атаки - основне завдання пасивної СВВ. Активний режим роботи присутній у «системи запобігання вторгнень », яка веде захисні дії в разі виявлення мережевої атаки.

Наявність даного режиму в програмному продукті є безумовною перевагою. Крім специфічних для СВВ характеристик варто відзначити такий

важливий фактор для порівняння як кросплатформеність. [3] Таким чином, наведемо характеристики, по яким був здійснений порівняльний аналіз роботи СВВ:

— вид виконання СВВ;
— метод визначення атак;
— наявність активного режиму;
— кросплатформеність.

Для порівняння обрані 4 найпопулярніших програмних продуктів СВВ: Snort, OSSEC, Suricata, AIDE.

Підсумки порівняння програмних продуктів представлені в таблиці 1.

Таблиця 1 – Порівняльна таблиця програмних продуктів СВВ

СВВ	Вид виконання	Метод визначення атаки	Активний режим	Підтримувані ОС
Snort	Мережева	Сигнатурний зі зворотним зв'язком	+	GNU/Linux, Windows
OSSEC	Хостова	Сигнатурний метод, пошук аномалій	-	Кросплатформеність
Suricata	Мережева	Сигнатурний зі зворотним зв'язком	+	GNU/Linux, Windows
Bro (Zeek)	Гібридна	Граф переходів, відповідний атаці	-	Unix, GNU/Linux

Таким чином, найбільш популярним методом виявлення мережевих атак є клас сигнатурних методів зважаючи на низький рівень помилкових спрацьовувань. Всі розглянуті рішення мають підтримку під ОС Linux, також існують СВВ з підтримкою ОС Windows. Кращими показали себе продукти Snort і Suricata. Їх метод визначення атаки - сигнатурний зі зворотним зв'язком, що дозволяє поліпшувати результат визначення найбільш часто виникають атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бірюков А.А. Інформаційна безпека. / А.А. Бірюков – М.: ДМК, 2017. – 434 с.

2. Система виявлення вторгнень. — Режим доступу: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень

3. Технології виявлення атак — Режим доступу: http://ypn.ru/448/intrusion-detection-technologies/