УДК 004.056.5
Породько М.Ю.[1], Лінець В.А.[1], Зайко Т.А.[2]
[1] студ. гр. КНТ-218 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц НУ «Запорізька політехніка»

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Зі збільшенням залежності світової економіки і державних структур від Інтернету, зростає і рівень ризику, пов'язаного із здійсненням мережевих атак. Здійснення атак через Інтернет стає потужним засобом ведення інформаційних війн між державами, вчинення злочинів у фінансовій та інших сферах, включаючи й акти тероризму. Згідно зі статистичними даними в першому кварталі 2017 року – 479 мільйонів комп'ютерних атак, а за аналогічний період 2018 року – 796 мільйонів атак. Подібне зростання атак з кожним роком потребує задіяння значно більших сил і витрат часу з боку адміністраторів і аналітиків безпеки. Складність логічної і фізичної організації сучасних мереж призводить до виникнення сучасної проблеми - об'єктивних труднощів при вирішенні питань управління та захисту від мережевих атак [1].

Через складнощі захисту мережевих ресурсів, на поточний момент дуже затребуваним напрямом в області забезпечення інформаційної безпеки є виявлення атак і запобігання вторгнень зловмисника в комп'ютерні системи і мережі. Для цього застосовується ряд спеціалізованих алгоритмів і засобів використовуваних для виявлення відомих і невідомих атак, а також методи виявлення аномальної активності, які ефективні для виявлення інсайдерських атак і атак «нульового дня».

При вирішенні завдань, пов'язаних з діагностикою та захистом мережевих ресурсів, центральним питанням є оперативне виявлення станів мережі, що призводять до втрати її працездатності, витоку інформації, збоїв, проникнення вірусів і інших погроз інформаційної безпеки. Раннє виявлення таких станів дозволяє своєчасно усунути їх причину та запобігти катастрофічним наслідкам.

Побудова шаблону нормальної поведінки аномаліїє трудомістким завданням і часто не завжди здійсненним. На практиці не кожна аномальна поведінка є атакою. Наприклад, адміністратор мережі може застосовувати

налагоджувальні утиліти, такі як ping, traceroute, mtr для діагностики мережного оточення. Подібні дії не мають нелегальних намірів, проте системи виявлення розпізнають цю діяльність як аномалію [2].

Під "аномалією", в даному тексті, мається на увазі відступ або ухилення від правила. Аналіз аномалій дозволяє виявляти відхилення трафіку мережевих пристроїв від «нормального» профілю. З результатів цього аналізу можна зрозуміти, що для виявлення аномалій в більшості випадків досить аналізувати основні параметри трафіку. При виявленні мережевої аномалії необхідно ретельно вивчити її природу, потенційну небезпеку та можливі наслідки, тобто вирішити задачу класифікації (тип джерела, причина та область виникнення, спосіб вияву, характер змін) [3].

Первинними даними для аналізу, при виявленні зловживань, є мережевий трафік. Виділені атрибути і поля мережевих пакетів передаються в модуль, який виконує пошук і перевірку на відповідність вхідних даних правилам і сповіщає про наявність загрози в разі позитивного спрацьовування одного з правил. Мережеві атаки є однією з причин аномальних явищ. Аномалії мережевого трафіку можуть стати причиною не коректної роботи мережі, призвести до відмови в роботі обладнання. Основними видами, на які діляться алгоритми виявлення мережевих аномалій, є: сигнатурні і поведінкові [2].

У сигнатурних алгоритмах застосовується підхід, при якому заздалегідь невідомо, які атаки можна очікувати і які з дій є аномальними. Перша стадія - самонавчання з метою побудови математичної моделі взаємодій. Після накопичення статистики, здійснюється прогноз роботи мережі в нормальних умовах. Друга стадія - розробка і застосування критеріїв, специфічних для застосовуваного статистичного підходу, що розділяють класифікатор мережевих процесів на нормальні і аномальні [4].

У поведінкових алгоритмах виконується складання списків правил, за якими приймаються рішення про порушення в роботі мережі. Такі правила засновані на використанні інформації про нормальну поведінку системи та порівнянні її з параметрами спостережуваної поведінки. В процесі своєї роботи система порівнює поточні показники активності з профілем нормальної діяльності, і у випадку значних відхилень може розглядатися як свідчення наявності атаки. Дані алгоритми характеризуються наявністю хибнопозитивних спрацьовувань, які пояснюються в першу чергу складністю точного і повного опису безлічі легітимних дій користувачів [2].

Отже, ідентифікація, діагностика та лікування аномалій - фундаментальна частина мережевих операцій і без них мережа не може ефективно і надійно функціонувати. Точне розпізнавання і дослідження аномалій в першу чергу залежить від надійності і своєчасності інформації, а по-друге, від використовуваних методів виявлення аномальних сигналів.

Швидке і точне виявлення аномалії мережевого трафіку - одна з неодмінних умов гарантуючих ефективну роботу мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Браницкий А.А. Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта 2018 год. [Электрон. ресурс] / А.А. Браницкий. – Режим доступа: http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2018/06/branitskiy_dissertation.pdf

2. Браницкий А.А. Анализ и классификация методов обнаружения сетевых атак 2016 год [Электрон. ресурс] / А.А. Браницкий, И.В. Котенко. – Режим доступа: http://www.mathnet.ru/php/getFT.phtml?jrnid=trspy&paperid=873&what=fullt&option_lang=rus

3. Микова С.Ю. Подход к классификации аномалий сетевого трафика из Международного научного журнала «Инновационная Наука» 2015 год [Электрон. ресурс] / С.Ю. Микова, В.С. Оладько, М.А. Нестеренко. – Режим доступа: https://cyberleninka.ru/article/n/podhod-k-klassifikatsii-anomaliy-setevogo-trafika/viewer

4. Шелухин О.И., Сравнительный анализ характеристик обнаружения аномалий трафика 2014 год [Электрон. ресурс] / О.И. Шелухин, А.П. Панкрушин. – Режим доступа: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-harakteristik-obnaruzheniya-anomaliy-trafika-metodami-kratnomasshtabnogo-analiza/viewer