УДК 004.891.3

ИНСТРУМЕНТЫ АКТУАЛИЗАЦИИ ПРАВИЛ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Попов Н.С. (Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»)
Научный руководитель – старший преподаватель Серебряков И.Е.
(Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»)

Быстрый рост технологий не только упрощает жизнь, но и создает множество проблем с безопасностью. С каждым годом развития интернета количество вредоносного траффика постепенно увеличивается. Система обнаружения вторжений (СОВ) является одним из основных средств защиты компьютерных атак. В моем докладе будут рассмотрены основные проблемы базовой СОВ и методы для их решения.

В настоящее время практически все крупные компании и государственные организации используют системы защиты от вторжений. Существует большое количество средств для решения данных задач. Для решения задач по защите от вторжений используются методы сигнатурного и эвристического метода обнаружения атак. Для поддержания работоспособности и актуальности, нужно постоянно обновлять базу решающих правил (БРП) и поддерживать ее актуальность, поскольку атаки видоизменяются, ведь достаточно небольших изменений чтобы сигнатура стала отличатся от тех что уже имеются в используемых правилах поиска.

Поставленную проблему необходимо решать в 2 этапа. В первую очередь нужно подключиться к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и создать модуль обновления набора правила путем получения БРП напрямую из ГосСОПКИ. Поскольку данная система создана по указу президента под руководством специальных служб и большого числа подключенных к этой системе предприятий, здесь можно найти одни из самых новых и актуальных сигнатур. Вторым этапом будет создание модуля для СОВ на основе искусственного интеллекта. Обучение предполагается сделать при помощи самого обширного набора данных KDD-99. Обучив один раз, позволит использовать систему вплоть до нового скопления данных. Позволяет находить новые, однотипные, измененные, частично скрытые и зашумленные атаки, дополняя сигнатурный поиск.

Данная система позволит использовать в полной мере проверенный годами сигнатурный метод поиска и внедрить современную систему способную закрыть собой оставшиеся недостатки и основываясь на найденных новым модулем пакетов формировать новые базы сигнатур и отправлять их в ГосСОПКУ.

Попов Н.С. (автор) Подпись

Серебряков И.Е. (научный руководитель) Подпись