УДК 004.056+343.98

МОДЕЛЬ ГРУППЫ АТАКУЮЩИХ ПРИ АНАЛИЗЕ ДАННЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Павлов А.В. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель – к.т.н., доцент Волошина Н.В.
(Университет ИТМО, г. Санкт-Петербург)

Выделение групп атакующих при анализе событий атак может позволить точнее определить уровень угрозы и применить адекватные ему меры. В работе представлена модель группы атакующих, основанная на данных систем обнаружения вторжений.

Введение. Подходы к анализу событий атак можно разделить на две группы – основанный на сети и основанный на атакующем. Первый подход основан на отслеживании изменения статуса активов с точки зрения безопасности, второй же нацелен на отслеживание действий конкретного атакующего в рамках множества атак.

Одной из задач при основанном на атакующем подходе является выделение групп атакующих. Выделение групп атакующих при анализе событий атак может позволить точнее определить уровень угрозы и применить адекватные ему меры. Оно позволяет соотнести события атак и предполагаемую группу, в чьих интересах они совершаются. Более того, при форензиологическом анализе оно позволяет выявлять ресурсы атакующих, не задействованные в конкретной атаке, но имеющие схожий шаблон с уже задействованными ресурсами. Тем не менее, существующие модели групп атакующих слишком абстрактны для применения в комплексных системах по выявлению групп атакующих и анализу их поведения.

Основная часть. В рамках работы рассмотрены характерные черты групп атакующих, на их основании построена модель. Проведена оценка возможности получения требуемой информации из данных систем обнаружения вторжений или на их основании методом обогащения данных через открытые источники.

Выводы. В результате работы представлена модель группы атакующих, основанная на данных, полученных из систем обнаружения вторжений. Модель может стать основой для создания комплексной системы по выявлению групп атакующих.

Павлов А.В. (автор) _____

Волошина Н.В. (научный руководитель) _____