УДК 004.056

АТРИБУТИВНЫЙ МЕТОД ВЫЯВЛЕНИЯ ГРУПП АТАКУЮЩИХ

Павлов А.В. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Волошина Н.В.
(Университет ИТМО)

В исследовании предлагается метод выявления групп атакующих на основании данных систем обнаружения вторжений. Метод основан на атрибутах и правилах. Проводится оценка эффективности метода на наборе данных CPTC-2018.

Введение. Выявление групп атакующих при анализе событий атак может позволить точнее определить уровень угрозы и применить адекватные ему меры. Более того, при форензиологическом анализе оно позволяет выявлять ресурсы атакующих, не задействованные в конкретной атаке. Выявление групп атакующих возможно осуществить на основании данных систем обнаружения вторжений.

Основная часть. В рамках метода предлагается три правила, по которым возможно произвести атрибутивное выявление групп атакующих:

1. Совпадение адресов источника атаки, если эти адреса относятся к публичным.
2. Совпадение адресов цели атаки при разнице временных меток не более 3 секунд.
3. Совпадение адресов цели и источника атаки при разнице временных меток не более 5 секунд.

Применение данных правил на наборе данных CPTC-2018 позволило получить высокую однородность и полноту кластеризации.

Выводы. Предложен метод выявления групп атакующих на основании атрибутов событий безопасности. Проведена экспериментальная оценка эффективности метода.