УДК 004.056.53

РАЗРАБОТКА МЕТОДОВ ОБНАРУЖЕНИЯ ЦЕЛЕВЫХ АТАК НА ОСНОВЕ АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калугина А.С. (Университет ИТМО)
Научный руководитель – к.т.н., Попов И.Ю.
(Университет ИТМО**)**

Разработан набор корреляционных правил и вспомогательных ресурсов для обнаружения атак на основе анализа анализа событий безопасности в SIEM-системах.

Введение. Постановка научной проблемы, описание существующего положения, анализ отечественного и зарубежного опыта в решении данной проблемы и т.д.

В настоящее время сохраняется тенденция роста сложности кибератак и возникают новые виды атак. Значительную опасность представляют целевые кибератаки (Advanced Persistent Threat, APT). Многие существующие и активно использующиеся методы и подходы к обнаружению целевых кибератак не справляются со своей задачей в таких условиях.

Основная часть. Суть предлагаемого решения без формул, таблиц, рисунков и использованных источников литературы; предложение оптимального решения поставленной проблемы, предложение оригинальных, экономичных, новейших методов исследований актуальных направлений.

Атаки оставляют следы в журналах событий безопасности на источниках, которые были задействованы при осуществлении целевой атаки, одно из решений этой проблемы заключается в централизованном сборе, сопоставлении и анализе журналов событий информационной безопасности затронутых устройств для выявления скрытых закономерностей, в том числе касающихся применения множества различных техник для последовательного выполнения атаки на конкретную систему.

Для достижения централизованного контроля журналов событий информационной безопасности применяется система управления событиями информационной безопасности – SIEM (Security Information and Event Management), которая предназначена для сбора событий с источников, их анализа и нахождения следов атаки.

Выводы. Описание практического использования результатов исследований, предложения по внедрению (испытание).

Своевременная реакция специалистов по информационной безопасности на атаку позволит значительно повысить защищенность системы в целом. Знание о структуре атаки и об этапе ее реализации, на котором находится злоумышленник, позволит не только эффективно и быстро отреагировать на вредоносное ПО или нарушение доступа, но и создать инструкции по недопущению аналогичных атак в дальнейшем, а также значительно сэкономить ресурсы при восстановлении системы к ее изначальному состоянию.

Калугина А.С. (автор)

Попов И.Ю. (научный руководитель)