УДК 004.056

ПОДХОД К ФОРМИРОВАНИЮ АДАПТИВНОЙ СИСТЕМЫ ЛОЖНЫХ ЦЕЛЕЙ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ АТАК

Шабала Е.Е (Университет ИТМО)
Научный руководитель – к.т.н, Менщиков А.А.
(Университет ИТМО)

Введение. Существующие средства защиты информации применяют различные методы и техники для выявления атак на ранних этапах развития. Большинство данных систем работают согласно заложенным правилам и некоторой эвристики, которая базируется на заранее выявленных зависимостях и паттернах поведения злоумышленника или реализации атак. Таким образом, данные системы защиты могут выявлять только известные атаки или же определять с определенной долей достоверности в том числе неизвестные атаки, если используются эвристические методы, машинное обучение. Для выявления паттернов и зависимостей используются сети и хосты приманки – honeypot. Они нацелены на привлечение злоумышленника, побуждение его к исследованию, и атаке целевого хоста. Записываемые при этом данные о механике атак, позволяют сформировать паттерны и тактики конкретного злоумышленника, скрипта, программного обеспечения, чтобы после применить эти данные для настройки средств защиты информации. Системы ложных целей, в отличии от honeypot позволяют обнаружить злоумышленника путем обмана и отвлечения [1]. Однако существует проблема, снижающая эффективность данных систем – легкость их обнаружения злоумышленником за счет формализованности ложных целей и отсутствии гибкости при их создании. Исследования в области разработки методов и алгоритмов создания адаптивных, динамических ложных целей являются крайне актуальными [2] и могут повысить как устойчивость систем к обнаружению, так и повысить эффективность управления ложными целями.

Основная часть. При помощи внедрения интеллектуальной мультисервисной архитектуры формируется подход к построению эффективной системы ложных целей, которая обладает высокой устойчивостью к обнаружению злоумышленником при осуществлении атак, используя механизм адаптивного управления приманками и ловушками. Кроме того, предложенный подход позволяет решить проблемы систем статических ложных целей, в частности статические ложные цели поддерживают только статическую обратную связь в ответ на запросы злоумышленника, что не дает возможность погрузить злоумышленника глубже в ловушку, в то время как адаптивные динамические ложные цели позволяют отвечать в соответствии с запросами злоумышленника.

Выводы. Предложен подход к формированию адаптивной системы ложных целей для выявления сетевых атак, позволяющий повысить защищенность как самой системы от обнаружения злоумышленником, так и защищаемой системы, путем более глубокого погружения злоумышленника в ловушки.

Список использованных источников:

1. Han X., Kheir N., Balzarotti D. Deception Techniques in Computer Security: A Research Perspective // ACM Computing Surveys. – 2019 – № 51(4). – С. 1-36.
2. Chiang C. -Y. J., Gottlieb Y. M., Sugrim S. J. ACyDS: An adaptive cyber deception system // MILCOM 2016 - 2016 IEEE Military Communications Conference. – 2016 – С. 800-805.