УДК 004.056

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ВЫСОКО-РАСПРЕДЕЛЕННЫХ DOS-АТАК МЕТОДОМ ОБМЕНА ПРЕДПОЛОЖЕНИЯМИ, ОСНОВАННЫМИ НА РЕЗУЛЬТАТАХ МОНИТОРИНГА НОВЫХ ПОДКЛЮЧЕНИЙ

Яресько С. Университет ИТМО
Научный руководитель – к.т.н., доцент ФБИТ Левко И.В.
Университет ИТМО

В данной работе рассмотрены проблемы обнаружения высоко-распределенных DoS-атак на компьютерную сеть, а также скорости и точности принятия решений агентами системы. Были проанализированы существующие решения и выявлены отличительные признаки высоко-распределенных DoS-атак, что позволило установить комплекс методов для мониторинга новых подключений в сети, обнаружения нестандартных активностей и дальнейшего принятия совместного решения по началу тревоги с применением мульти-агентного подхода для увеличения скорости и точности обнаружения.

Введение. Высоко-распределенные DoS-атаки частично или полностью нарушают доступность информационной системы, используя определенные ограничения пропускной способности сети. Существующие системы и методы обнаружения данного вида атак в большинстве случаев основываются на мониторинге объема трафика, получаемого жертвой атаки, однако, из-за характерной нестабильности трафика, резкое увеличение его объема может быть ошибочно распознано как вредоносная атака. Также важными проблемами являются скорость и точность распознавания атаки, так как необходим некий промежуток времени на анализ трафика, что повышает риски и дает преимущество атакующему.

Основная часть. Предлагаемая система обнаружения базируется на характерной особенности высоко-распределенных DoS-атак – большом количестве новых IP-адресов в сети. Мониторинг новых подключений и обнаружение нестандартных активностей в сети осуществляется с использованием статистического подхода и алгоритма кумулятивной суммы. Анализируя входящие подключения в индивидуальных транзитных сетях, агенты системы, согласно заданному правилу, делают предположения о начавшейся атаке. В результате комбинирования данных распределенных предположений выносится, согласно заданному правилу, совместное решение о начале тревоги.

Выводы. Программная симуляция работы системы позволила определить оптимальное количество агентов в системе, а также подтвердить увеличение скорости распознавания благодаря использованию мульти-агентного подхода. Данная система может быть применена как самостоятельное решение для обнаружения высоко-распределенных DoS-атак, так и в качестве компонента для комплексной системы защиты компьютерной сети. Дальнейшее исследование позволит повысить точность распознавания, а также сократить время на обнаружение атаки и принятие решения.

Яресько С. (автор) Подпись
stepan_yaresko@mail.ru

Левко И.В. (научный руководитель) Подпись