УДК 004.352.4.056.53

ХАРАКТЕРНЫЕ ИЗМЕРЕНИЯ ПОКАЗАТЕЛЕЙ АТАКИ СЕТЕВОГО СКАНИРОВАНИЯ

Ульянов М.В. студент гр. ИТб-121, IV курс
Научный руководитель: А.В. Протодьяконов, к.т.н., доцент
Кузбасский Государственный Технический Университет
имени Т.Ф. Горбачева
г. Кемерово

При изучении задач обнаружения вторжений или атак в сети часто рассматривается тесно связанный с этой проблемой вопрос аномальной активности или аномалий в параметрах сетевых взаимодействий. Связь между этими двумя явлениями, безусловно, существует, но не следует считать их эквивалентными, т.е. не все аномалии стоит рассматривать как атаки и не все атаки сопровождаются аномалиями. Это можно проследить на достаточно простых примерах. Существует эффект мощного всплеска посещаемости определенного web-ресурса при проявлении ссылки на другом web-ресурсе, имеющем большую популярность. Атакой такая активность не является, однако аномальное поведение будет зафиксировано. Другой пример: пароль пользователя для доступа к ресурсу был похищен или каким-либо образом скомпрометирован. В этом случае для реализации атаки нет необходимости посылки большого количества пакетов. Аномалия в данном случае замечена не будет. В связи с этим необходимо разделять понятия атак и аномального поведения и рассматривать их не как одно целое, а как дополняющее друг друга события в процессе обнаружения нежелательных воздействий.

Принимая во внимание разделение понятий атак и связанных с ними аномалий в сетевом трафике, можно тем не менее установить некоторое соответствие между этими явлениями. Не прибегая к сложным расчетам, можно привести качественные примеры, отражающие подробную связь. Так, DOS- или DDOS- атаки без использования каких-либо уязвимостей в программном обеспечении характеризуются большим количеством пакетов на доступные ресурсы. Атака по подмене таблицы маршрутизации использует большое количество агр-пакетов для подмены элементов таблиц, далее большое количество пакетов, которое может быть принято за аномалию, уже не требуется. Атаки подбор паролей также

имеют отличное от других атак аномальное поведение. В данном случае – на прикладном уровне стека протоколов. Таким образом, уже известные атаки, их конкретные реализации имеют определенные свойства и не только при рассмотрении сетевого взаимодействия, но и различные параметры аномального поведения.

Сканирование сетевых ресурсов.

Одним из видов сетевых атак является сканирование. Сама по себе такая атака не несет какой либо угрозы, однако на основании информации, полученной при сканировании, могут происходить другие атаки.

Обнаружение сканирования, в отличие от обнаружения вредоносных воздействий, представляет особый интерес. Он заключается в том, что существует очень неявная граница того, чем отличается нормальное поведение системы от аномального, т.е. обусловленного действиями злоумышленника, пытающегося получить информацию о других узлах в сети. Тонкость состоит как раз в том, что сканирующие пакеты замаскированы или замешаны во множестве обычных и необходимых для работы сети пакетов. Существуют различные методы обнаружения сканирования. Наиболее простым способом является проверка превышения количества пакетов от определенного узла некоторого наперед заданного порогового значения за единицу времени. Такая проверка выполняется для определения факта сканирования в такой распространенной системе обнаружения вторжения, как Snort. Естественно, в случае используется вполне определенная модель сканирования: один узел-нарушитель собирает информацию о многих узлах в сети. Также делается допущение, что интенсивность сканирования достаточно высока, по крайней мере превышает значения интенсивности обмена данными(пакетами) в нормальном режиме между узлами сети.

Для оценки наличия или отсутствия сканирования выберем измеримую величину, которая измеряется в случае наличия сканирующих пакетов во множестве всех сетевых пакетов. Пусть такой величиной будет энтропия. По определению,

$$H = -\sum_{i \in I} p_i \log p_i,$$

Где, H – энтропия; I – множество возможных сетевых взаимодействий узлов; p_i – вероятность данного взаимодействия i.

Вывод: В настоящее время любое отклонение трафика от нормального, превышающего порог, в большинстве систем обнаружение считается атакой в аномалии можно повысить достоверность определения именно атаки, а также снизить процент ложных срабатываний.

Список литературы:

1. Макаров А.С., Фадин А.А., Цирлов В.Л. «Средства и технологии анализа защищенности.» / Информационное противодействие угрозам терроризма. 2005
2. Макаров А.С., Миронов С.В., Цирлов Л.В., «Опыт тестирования сетевых сканеров уязвимостей.» 2011 .