Секция «Вычислительная математика и кибернетика»

Применение метода временных рядов для определения влияния DDoS-атак на системный и сетевой трафик сервера

Левоневский Дмитрий Константинович
Студент
Санкт-Петербургский государственный электротехнический университет "ЛЭТИ Компьютерных технологий и информатики, Санкт-Петербург, Россия
E-mail: DLewonewski.8781@gmail.com

В настоящее время в Интернете распространены атаки типа «Distributed Denial of Service (DDoS)», ставящие своей целью вывести объект (вычислительную систему) из рабочего состояния. Масштабные DDoS-атаки в большинстве случаев приводят к финансовым потерям со стороны жертвы, а также отличаются простотой организации и высокой эффективностью. Эти особенности обусловливают актуальность исследования DDoS-атак. В частности, представляет интерес статистическое исследование временных рядов системного и сетевого трафика как в различных режимах работы сервера, что позволяет в дальнейшем выявлять факт вторжения на основе поведенческих сигнатур.

Для исследования временных рядов был разработан стенд, моделирующий клиент-серверное взаимодействие между компьютерами как в регулярном режиме, так и при наличии наиболее распространённых атак (HTTP-flood, SYN-flood, UDP-flood). Стенд включает в себя средства генерации трафика на клиентской стороне и средства мониторинга – на сервере. Для генерации атак использована программа Longcat Flooder, для генерации регулярного трафика разработана программа Client. Для сбора данных разработана утилита Monitor, протоколирующая объём входящего и исходящего сетевого трафика и загрузку памяти и процессора. В качестве атакуемого хоста выбран Web-сервер на базе Apache/PHP/MySQL.

Визуальный анализ гистограмм, снятых со стенда в разных режимах работы, говорит о различиях в распределениях измеряемых параметров при наличии и отсутствии атак. Это выражается качественно в изменении закона распределения и количественно в изменении его параметров – выборочных среднего, дисперсии и коэффициента асимметрии. В ходе работы были проверены статистические гипотезы о законах распределения и произведён расчёт статистических оценок их параметров для всех измеряемых параметров в четырёх режимах работы стенда, что позволило сравнить эти режимы. Например, для атаки класса HTTP-flood результаты говорят:

- о повышении дисперсии загрузки памяти при наличии атаки;
- об изменении закона распределения времени простоя процессора;
- о снижении дисперсии входящего и исходящего сетевого трафика.

Результаты проведённых исследований можно использовать для разработки системы обнаружения вторжений. При этом необходимо учитывать, что целевые компьютерные системы значительно отличаются по мощности и нагрузке, что приведёт к изменению параметров распределений. Поэтому целесообразно перед внедрением построить

шаблон штатного функционирования системы для фиксации отклонения и обеспечения защиты в реальном времени.

Данная работа выполнена при поддержке компании «ИнфоТеКС Академия».

Литература

1. 1. Бриллинджер Д. Временные ряды. Обработка данных и теория. – М.: Мир, 1980. – 536 с.

2. 2. Петров В.В. Статистический анализ сетевого трафика. – М.: МЭИ, 2003. – 47 с.

3. 3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2006. – 958 с.