УДК 681.3.053

МОДЕЛИРОВАНИЕ DDOS-АТАК ТИПА HTTP-FLOOD И SLOWBODY (RU-DEAD-YET) С ПОМОЩЬЮ СРЕДСТВА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ СМО – GPSS WORLD

© 2017 М. С. Бондаренко

Воронежский институт высоких технологий (г. Воронеж, Россия)

Распределенные атаки отказа в обслуживании (DDoS) являются наиболее распространенным и самым эффективным средством в арсенале злоумышленников. Атаки такого вида имеют широкий спектр областей применения, а также подходов и средств для их реализации. Для исследования различных методов реализации DDoS-атак и получения статистических данных можно представить Web-сервер в виде системы массового обслуживания (СМО) и использовать средства имитационного моделирования, такие как GPSS-World. GPSS является языком имитационного моделирования, который позволяет наглядно показать ключевые места СМО и получить статистические данные по результатам моделирования исследуемого объекта.

Ключевые слова: DDoS, атака, Web-сервер, модель, GPSS, СМО.

Во время исследования реальных объектов нашего мира зачастую приходится исследовать не сам объект, а его модель. Модели реальных объектов создаются путем упрощения их свойств и представлением в необходимой форме, в зависимости от потребностей конкретного исследования. Моделирование используют в тех случаях, когда исследование самого объекта не целесообразно или же попросту невозможно, например изучение космического пространства или поведение ядерной реакции. Для моделирования технических объектов зачастую используется математический аппарат алгебраических и дифференциальных уравнений, а также алгебру логики. Математические модели подразделяются на аналитические и имитационные. Аналитические модели представляют собой набор уравнений или систем уравнений, записанных в виде алгебраических, дифференциальных, а также интегральных соотношений. Этот тип моделей применяется для описания фундаментальных свойств реальных объектов, поскольку фундамент прост по своей сути. Сложные объекты зачастую невозможно описать аналитически.

Отличие имитационных моделей от аналитических заключается в том, что вместо набора уравнений имитационные модели строятся на основе алгоритма, описывающего последовательность развития процессов внутри объекта исследования, после чего фиксируют значения процессов на определенных этапах моделирования. Имитационное моделирование характеризуется сочетанием двух факторов – неопределенности и возможности ветвления процессов в зависимости от конкретных реализаций этой неопределенности [1]. На сегодняшний день, когда услуги являются полноценным товаром, а качество обслуживания играет ключевую роль в технических, политических, социальных и коммерческих системах, часто объектом моделирования становятся системы массового обслуживания (СМО). Системами массового обслуживания называют те системы, в которых случайным образом возникают заявки и существуют устройства для их обработки. При имитационном моделировании события внутри системы происходят с течением обусловленного промежутка времени и его индикатором – транзактом. Количество транзактов теоретически не ограничено, но в определенный промежуток времени активным может быть только один транзакт, который вызывает какое либо событие. Физический смысл транзакта может принимать любые формы, такие как люди, сигналы, внешние воздействия и т. д. Имитационная модель может проследить траектории прохождения транзактов при различных условиях и собрать статистические данные о них.

Поскольку речь в данной работе идет об атаках направленных на отказ в обслуживании веб-серверов, то объектом моделирования в рамках данной работы будет выступать непосредственно веб-сервер. Поскольку основной задачей сервера является прием запросов их обработка и ответ на них, то сервер можно представить в виде классической системы массового обслуживания.

Бондаренко Михаил Сергеевич – Воронежский институт высоких технологий, магистрант, e-mail: mikhailbondarenko2017@yandex.ru.

Классическим инструментом для имитационного моделирования СМО является программная среда GPSS World. GPSS предназначен для моделирования СМО и аналогичных им систем, и имеет для данных целей специальные операторы, синтаксис, а также вспомогательные инструменты. При разработке GPSS впервые применялся объектно-ориентированный подход. Именно в GPSS впервые было введено понятие «транзакт» и другие понятия теории массового обслуживания. Каждый оператор GPSS представляет собой целую систему, которая выполняет внутри себя набор функций, который внешне ни как не проявляется, среди таких функций можно выделить сбор статистики о транзактах, ее обработка, изменение параметров транзакта. Все это говорит о том, что среда моделирования GPSS World, лучше всего подойдет для реализации задач моделирования веб-сервера как СМО.

Для моделирования в рамках исследования были выбраны методы реализации атак, направленных на отказ в обслуживании Slowbody (RUDY) и HTTP-flood. Для анализа непосредственно механизмов атак этих видов, модели серверов были существенно упрощены относительно реальных веб-серверов, в которых параллельно на ресурсы влияет еще целый ряд сторонних факторов. Основными ресурсами сервера были выделены три составляющих, таких как программный буфер очереди, который является параметром программной реализации веб-сервера, а также аппаратные составляющие веб-сервера, такие как объем ОЗУ и вычислительная мощность ЦПУ.

Первой мы смоделируем реализацию технологии HTTP-flood. Пусть при нормальном режиме работы веб-сервер получает запросы, распределенные по экспоненциальному закону с интенсивностью равной 10 запросам в секунду. Буфер очереди сервера равен 1000 одновременных соединений, объем оперативной памяти составляет 8 гигабайт, а вычислительная мощность процессора обусловлена приблизительным временем обработки одного запроса, которое равно 350 миллисекунд, модельное время составляет 1 минуту. При моделировании поток запросов сперва попадает в очередь, которая является буфером одновременных подключений, после чего занимает ресурсы оперативной памяти и попадает на обработку в ЦПУ. Затем запрос освобождает ресурсы и удаляется из модели, так как по логике он был отправлен клиенту и покинул пределы модельного пространства, а затем цикл действий повторяется для следующего запроса. При условии, что количество запросов превышает объем свободного места в очереди, эти запросы получают отказ на обслуживание и отбрасываются. Листинг модели представлен в приложении А. На рисунке 1 показан отчет системы GPSS World по итогам моделирования.

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	596	0	0
	2	TEST	596	0	0
	3	QUEUE	596	0	0
	4	ENTER	596	0	0
	5	DEPART	596	437	0
	6	SEIZE	159	0	0
	7	ADVANCE	159	1	0
	8	RELEASE	158	0	0
	9	LEAVE	158	0	0
	10	TERMINATE	158	0	0
LBL	11	SAVEVALUE	0	0	0
	12	TERMINATE	0	0	0
	13	GENERATE	1	0	0
	14	TERMINATE	1	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
CPU	159	1.000	377.251	1	160	0	0	0	437

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
BUF	1	0	596	596	0.000	0.000	0.000	0

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
RAM	8192	7316	0	876	1192	1	438.297	0.054	0	0

Рисунок 1. Отчет по итогам моделирования нормальной работы веб-сервера

Как видно из отчета, сервер справился с этой нагрузкой, и у нас нет пакетов, которым было отказано в обслуживании, единственное скопление пакетов наблюдается при выходе из буфера очереди и занятии процессора, что может говорить о том, что вычислительную мощность процессора следует увеличить.

На следующем этапе смоделируем атаку на веб-сервер с использованием технологии HTTP-flood. Условия остаются прежними, за исключением интенсивности входящих запросов, которая при атаке будет приближенно равна 200 запросам в секунду. Отчет по результатам моделирования представлен на рисунке 2.

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	9887	0	0
	2	TEST	9887	0	0
	3	QUEUE	5260	1001	0
	4	ENTER	4259	0	0
	5	DEPART	4259	4095	0
	6	SEIZE	164	0	0
	7	ADVANCE	164	1	0
	8	RELEASE	163	0	0
	9	LEAVE	163	0	0
	10	TERMINATE	163	0	0
LBL	11	SAVEVALUE	4627	0	0
	12	TERMINATE	4627	0	0
	13	GENERATE	1	0	0
	14	TERMINATE	1	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
CPU	164	1.000	365.847	1	165	0	0	0	4095

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
BUF	1001	1001	5260	4156	528.955	6033.710	28747.569	0

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
RAM	8192	0	0	8192	8518	1	6466.246	0.789	0	1001

SAVEVALUE	RETRY	VALUE
DENIAL	0	4627.000

Рисунок 2. Отчет по результатам моделирования атаки HTTP-flood на сервер

В отчете наглядно отражен принцип работы данного метода атаки, явно выражено переполнение буфера подключений, а так же большой объем ОЗУ занят в очереди на обработку в ЦПУ. По итогу моделирования данного вида атаки, наглядно представлен принцип переполнения ресурсов сервера, а также видны «узкие» места в ресурсах. Из 9887 запросов отправленных за минуту на сервер, было обработано всего 163 запроса, 4627 запросов получили отказ на обслуживание, остальные же запросы просто занимают ресурсы сервера. Очевидно, что в реальных условиях серверы имеют большие объемы ресурсов, а также имеют инструменты защиты от такого рода атак. Но в реальных условиях при массовых распределенных атаках количество запросов существенно превышает модельные параметры. А при наборе дополнительных технологий и методов трафик этих атак способен обходить существенное количество слоев защиты, и попутно перегружать устройства защиты, находящиеся перед сервером, такие как межсетевые экраны и маршрутизаторы, что говорит об огромном потенциале этих атак, и их актуальности за счет простоты и дешевизны их реализации, относительно направленных атак.

На следующем этапе мы построим модель атаки основанной на технологии Slowbody (RUDY). Суть данной атаки заключается в занятии ресурсов сервера относительно небольшим количеством запросов, но длительным по обработке каждого из них. При реализации данной атаки на сервер приходит запрос типа POST, который в заголовке содержит объем передаваемой сервером информации, под который сервер выделяет ресурсы, а далее ожидает получения

всех байтов информации указанных в первом пакете запроса. Весь объем информации дробится на кадры размером по 1-2 байта, и отправляется на сервер с задержкой равной 1-2 секундам, ввиду чего уже занятые ресурсы сервера вынуждены долгое время простаивать до получения полного объема данных. Составим набор условий к модели.

Пусть интенсивность потока заявок к серверу равна 100 запросов в секунду и распределена по экспоненциальному закону. Буфер очереди сервера равен 1000 одновременных соединений, объем оперативной памяти составляет 8 гигабайт, а вычислительная мощность процессора обусловлена приблизительным временем обработки одного запроса, которое равно 350 миллисекунд, модельное время составляет 1 минуту. Каждый запрос равен 48 байтам данных, а интервал задержки между получением соседних байтов данных равен 1-2 секундам.

В виду специфики данного вида атаки, а так же инструментов реализации моделей на GPSS, придется прибегнуть к некоторым допущениям. Поскольку в GPSS и теории СМО транзакт является не делимой атомарной единицей, а по технологическим условиям атаки каждый запрос делится на количество байтов данных, каждый из которых имеет свою задержку, мы вынуждены прибегнуть к блоку языка GPSS – «SPLIT». При входе транзакта в данный блок, блок SPLIT создает указанное в первом параметре количество копий этого транзакта, после чего оригинал отправляется дальше по блокам программы, где задерживается до получения сигнала, а копии транзакта перенаправляются в блок с меткой, указанной во втором параметре блока SPLIT. После чего обрабатываются в отдельной ветке программы, после чего удаляются, а в основную ветку программы подается сигнал о разрешении движения транзакта – оригинала, что в совокупности создает задержку обработки в совокупности, отражающую ожидание всех битов запроса, а также задержку на обработку всего запроса. В роли битов разделенного запроса в модели фигурируют копии транзактов, пришедших в виде запросов на сервер.

Отчет по результатам выполнения модели представлен на рисунке 3.

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	5926	0	0
	2	TEST	5926	0	0
	3	QUEUE	5104	1001	0
	4	ENTER	4103	0	0
	5	DEPART	4103	4095	0
	6	SEIZE	8	0	0
	7	ASSIGN	8	0	0
	8	SPLIT	8	1	0
	9	TEST	7	0	0
	10	ADVANCE	7	0	0
	11	RELEASE	7	0	0
	12	LEAVE	7	0	0
	13	TERMINATE	7	0	0
LBL	14	SAVEVALUE	822	0	0
	15	TERMINATE	822	0	0
	16	GENERATE	1	0	0
	17	TERMINATE	1	0	0
WAITH	18	ADVANCE	376	1	0
	19	ASSEMBLE	375	1	0
	20	SAVEVALUE	7	0	0
	21	TERMINATE	7	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
CPU	8	1.000	7499.786	1	56	0	0	0	4095

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
BUF	1001	1001	5104	4101	223.778	2630.620	13386.524	0

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
RAM	8192	0	0	8192	8206	1	5346.509	0.653	0	1001

Рисунок 3. Отчет по результатам моделирования метода атаки Slowbody (RUDY)

Из отчета по результатам моделирования отчетливо виден принцип работы метода атаки Slowbody (RUDY). При вдвое меньшей интенсивности запросов мы имеем существенное количество отказов в обслуживании. Из 5926 запросов отказано в обслуживании 822 запросам, а обработано всего 7 запросов, остальное же запросы занимают буфер очереди, и оперативную память в очереди к процессору. По итогу моделирования атаки типа Slowbody (RUDY) можно сказать, что атаки данного рода гораздо более эффективны и трудно обнаруживаемы, ввиду того, что не требуют большого количества трафика, и не так сильно выражаются при мониторинге ресурсов сервера.

ЛИТЕРАТУРА

1. Бронов, С. А. Имитационное моделирование: учеб. пособие / С. А. Бронов; ФГОУ ВПО «Сибирский федеральный университет», кафедра «Системы автоматизированного проектирования». – Красноярск: СФУ, 2007. – 82 с.

MODELING DDOS-ATTACKS SUCH AS HTTP-FLOOD AND SLOWBODY (RU-DEAD-YET) BY MEANS OF SIMULATION SMO – GPSS WORLD

© 2017 M. S. Bondarenko

Voronezh Institute of High Technologies (Voronezh, Russia)

Distributed denial of service (DDoS) are the most common and most effective tool in the arsenal of criminals. Attacks of this kind have a wide range of applications, as well as approaches and tools for their implementation. To investigate various methods for implementing DDoS attacks and obtaining statistical data, it is possible to present a Web server in the form of a queuing system (QMS) and use simulation tools such as GPSS-World. GPSS is a simulation language that allows you to visually show the key places of the SMO and obtain statistical data from the simulation results of the object under study.

Keywords: DDoS, attack, Web-server, model, GPSS, QMS.