УДК 004.056.5:004.7

студент Е.И. Грушко
ГВУЗ "Национальный горный университет"

СОВРЕМЕННАЯ СЕРВЕРНАЯ АРХИТЕКТУРА "FRONT AND BACK ANDS" КАК СРЕДСТВО ПРОТИВОДЕЙСТВИЯ АТАКАМ ТИПА DDOS SYN-FLOOD И SLOW-POST

В данной работе рассматриваются распределенные атаки типа "отказ в обслуживании", направленные на использование уязвимостей программного кода веб-сервера. Рекомендуется использовать архитектуру работы сервера "Front and back ends" как метод активной защиты от атак DDoS Syn-Flood и Slow-Post.

Развитие информационных технологий, активное внедрение компьютеров во многие сферы деятельности человека обуславливает появление технического прогресса, а вместе с тем и развитие новых угроз информационной безопасности, формирование новых атак, направленных на информационные ресурсы. Одной из самых актуальных проблем на сегодня является защита веб-ресурсов от DDoS (англ. "Distributed Denial of Service") атак.

Для компаний, где электронная коммерция является основой бизнеса одной из самых опасных атак является DDoS. Злоумышленники атакуют торговые площадки не столько с целью вымогательства, сколько с целью скрыть следы в ходе проведения мошеннических транзакций. Чаще всего при таких схемах финансовые ресурсы теряют как сами организации, так и их клиенты. Поэтому устойчивость сервиса к DDoS-атакам является одним из факторов, определяющих его репутацию.

DDoS (от англ. Distributed Denial of Service, отказ в обслуживании) – атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (сайтам), либо этот доступ затруднён. Данная атака направлена на нарушения такого свойства информации как доступность.

Slow Post DDoS – один из видов атак, который базируется на уязвимости в протоколе HTTP. Уязвимо поле Content-Length POST запроса, которое

позволяет веб-серверу оценить какой объём данных к нему поступает. Как только заголовок отправлен, тело POST запроса начинает передаваться с очень медленной скоростью, что позволяет использовать ресурсы сервера намного дольше, чем это необходимо, и, как следствие, помешать обработке других запросов. Несколько тысяч таких соединений могут сделать недоступным веб-сервер для легитимных пользователей.

По данным ЗАО «Лаборатория Касперского» одним из самых распространённых видов DDoS атак является Syn-flood DDoS, в ходе которой сервер получает от зараженных злоумышленником персональных компьютеров множество запросов на установку TCP-соединения. При этом злоумышленники с помощью манипуляций с пакетами не устанавливают соединения до конца, и они занимают ресурсы системы. Из-за того что очередь соединений ограничена, а компьютеры участвующие в атаке могут генерировать запросы с очень большой скоростью, через некоторое время после начала атаки сервер не может принимать подключения от легитимных пользователей[1].

Проанализировав работу веб-сервера Apache, кроме его достоинств, заявленных разработчиками с точки зрения информационной безопасности обнарнужен ряд проблем:

– основная проблема Apache – на каждый запрос клиента выделен отдельный процесс (как минимум – поток), который так же может быть нагружен различными модулями и потребляет достаточно большое количество ресурсов. Кроме того, этот процесс будет “висеть” в памяти операционной системы до тех пор, пока не передаст весь запрашиваемый контент клиенту. Из этого следует, что данный недостаток может быть использован злоумышленником для организации Syn-flood DDoS атаки;

– если у пользователя скорость канала связи не большая, а контент достаточно объемный, то процесс обработки запроса может занять длительное время. Например, сервер генерирует контент за 0,1 сек, а передавать его пользователю будет 10 сек, все это время занимая системные

ресурсы. Следовательно, этот недостаток может использоваться злоумышленниками для проведения Slow-Post DDoS атак.

Обобщенные термины “Front end” и “Back end” указывают на начальную и конечную стадию процесса в двухуровневой конфигурации веб-серверов. “Front-End” – это открытая часть проекта, обеспечивающая прием запросов от пользователей, трансляцию запросов к “Back-End” и выдачу непосредственного содержимого пользователю. “Back-End” – это исполнительная часть системы, которая обеспечивает выполнение PHP-скриптов, формирование контента и работу бизнес-логики приложений.

Такая серверная архитектура была предложена ведущими инженерами, работающими с серверным программным обеспечением, для организации сложных высоконагруженных проектов, которые обслуживают несколько тысяч клиентов в секунду. По такой схеме работают социальные сети “Вконтакте”, “Facebook” и другие популярные веб-ресурсы[2].

В результате проведенных исследований для обеспечения защиты сервера Apache от рассмотренных уязвимостей предлагается построить систему на базе программного обеспечения сервера связки Nginx + Apache. Использование такой связки серверов называется “Front and back ends” серверной архитектурой, где Nginx - это “Front-End” сервер обрабатывающий первичные запросы клиентов, и служащий Proxy сервером между клиентом и основным сервером Apache, используемым как “Back-End” сервер, который непосредственно создает контент веб-системы.

Установлено, что серверная архитектура типа “Front and back ends” эффективно защищает сервер от типа атак DDoS направленных на ошибки в программном коде серверного обеспечения, а именно распределенных атак отказа в обслуживании Syn-flod и Slow-Post . Предложенный вариант защиты сервера является финансово экономным так как используется программное обеспечение с типом лицензии “GNU General Public License”. Следовательно, бизнес может экономить значительные средства и эффективно противостоять данным атакам при борьбе с злоумышленниками.

Рассмотренные атаки являются частью класса атак DDoS, направленных на ошибки в программном коде веб-сервера Apache. Следует заметить, что для атак типа DDoS, направленных на снижение пропускной способности сетевой инфраструктуры на сегодняшней день не существует эффективных методов и средств защиты. Это связано с архитектурой компьютерной сети, а именно с тем, что она имеет ограниченную пропускную способность, которая при использовании мощной DDoS атакой полностью “засоряется”, и как следствие доступ для легитимных пользователей к серверу становится невозможным. Таким образом, рассмотрена частичная защита от действий злоумышленников, которая будет эффективна только при условии, что суммарная мощность атаки на сетевую инфраструктуру будет меньше, чем пропускной канал сервера и достаточной для обработки запросов от легитимных пользователей.

Перечень литературы:

1. URL: http://www.securelist.com/ru/analysis/208050712/Obzor_DDoS_ atak_vo_vtor om_kvartale_2011_goda - “Обзор DDoS-атак во втором квартале 2011 года”.

2. URL: http://habrahabr.ru/blogs/sysadm/108211/ - “apache+nginx+ gzip_static+ yuicom pres