УДК 004.(491+738.5.057.4):65.012.8

СЕТЕВАЯ АТАКА SYN-FLOOD

Прокопчук А.Е., Баранов А.А.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, alex0392@gmail.com

В данной работе рассмотрена сетевая атака «Отказ в обслуживании» и ее разновидность SYN-FLOOD, а так же принципы ее работы и механизмы защиты.

Ключевые слова – Syn-flood, RFC 4987, защита, DoS.

ВВЕДЕНИЕ

SYN-флуд – одна из разновидностей сетевых атак типа отказ от обслуживания, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок.

Традиционные "SYN flooding DoS" атаки работают по двум принципам:

- "one-on-one" одна машина отсылает достаточное количество SYN-пакетов, чтобы заблокировать доступ к серверу.
- "many-on-one" множество программ зомби, установленных на разных серверах, атакуют целевую машину SYN пакетами.

ПРИНЦИП АТАКИ

Заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения, ожидающие подтверждения от клиента.

По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого легитимные клиенты не могут установить связь, либо устанавливают её с существенными задержками.

МЕХАНИЗМ ЗАЩИТЫ

- **Стандартный таймаут**. Полуоткрытые соединения по прошествии некоторого времени выбрасываются из буфера. При истощении буфера запросы клиентов на подключение будут проходить с вероятностью C1/C2, где C1 – количество SYN-пакетов от клиента, C2 – количество SYN-пакетов от всех остальных (включая атакующего). Даже при нагрузке на канал атакующего в 6 пакетов в секунду C1/C2 – примерно 1/100, т.е. служба выведена из строя на 99%.
- **Без лимитный буфер полуоткрытых соединений**. При нагрузке на канал атакующего 100Mb/сек и таймауту около минуты очередь полуоткрытых соединений будет занимать примерно 1 Gb памяти, что для крупных серверов не смертельно. Побочный эффект: атакуемый сервер отвечает трафиком, в 3 раза большим, чем трафик атакующего (говорят, что происходит DDoS с умножением в 4 раза), что может привести к истощению пропускной способности канала. Однако, при невозможности истощить ширину канала, защита от атаки будет абсолютной, ни одно клиентское соединение не будет отвергнуто.
- **Очистка наиболее старых полуоткрытых соединений**. При переполнении буфера из него удаляется самое старое полуоткрытое соединение. Побочный эффект: если при атаке буфер заполняется за время t, то клиент не сможет подключиться во время атаки, если время подтверждения соединения больше t – его запрос тоже будет выброшен. Например, для нагрузки канала атакующего 4Мбит/сек и длины буфера 512 время t – около 50 мс, что гарантированно отбросит все попытки подключения к серверу с dialup и многие – с выделенных линий. Увеличивая размер буфера, защиту можно свести к предыдущему варианту.
- **SYN COOKIE**. После истощения буфера информация, которая не помещается в буфер, отсылается клиенту, который якобы запросил ее. Если клиент – настоящий, то он возвращает информацию обратно, если поддельный – она теряется, причем механизм реализован в рамках RFC по TCP, т.е. его поддерживают и клиенты, не знакомые с этой технологией. Операционная система с SYN COOKIE, независимо от размера буфера полуоткрытых соединений, совершенно неуязвима для SYN-flood атак. Побочный эффект: запрет "больших окон".

ВЫВОДЫ

SYN-flood атака морально устарела, так как на сегодняшний день существуют эффективные методы устранения атаки. Сегодня может использоваться в лучшем случае в качестве обычной flood-атаки на превышение пропускной способности канала связи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. SYN-флуд (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/SYN-флуд.
2. TCP SYN Flooding Attacks and Common Mitigations RFC 4987 (Электрон. ресурс) / Способ доступа: URL: http://tools.ietf.org/html/rfc4987.
3. Атака SYN-flood (Электрон. ресурс) / Способ доступа: URL: http://hpc.name/text/get/635/p1.html.
4. Syn-flood атака – практика (Электрон. ресурс) / Способ доступа: URL: http://www.securitylab.ru/analytics/216198.