УДК 004.492.3

ПРОЕКТИРОВАНИЕ СЕРВИСА ОБНАРУЖЕНИЯ РАСПРЕДЕЛЕННЫХ СЕТЕВЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

М.Ю. МАКАРЫЧЕВ, В.А. МАКАРЫЧЕВА
(Представлено: канд. техн. наук, доц. А.Ф. ОСЬКИН)

В данной статье рассматривается проект сервиса обнаружения DDoS-атак (ICMP-flood, UDP-flood, TCP-SYN-flood). Выделены основные подсистемы сервиса и установлено взаимодействие между ними.

Введение. При обеспечении защиты сетевых ресурсов, основной задачей является своевременное обнаружение состояний сети, приводящих к частичной или полной потере ее работоспособности, искажению, уничтожению или утечке информации. Оперативное обнаружение таких состояний позволит устранить их причину и предотвратить возможные последствия угроз информационной безопасности. Актуальность темы подтверждается сложностью обнаружения атак типа «отказ в обслуживании», т.е. DoS (Denial of Service) или DDoS-атак (Distributed Denial of Service). Во-первых, они не направлены на уязвимости, которые могут быть исправлены, во-вторых, каждый отдельный пакет, отправляемый на компьютер жертвы, является вполне легитимным, в-третьих, такие атаки носят продолжительный характер – от нескольких часов до нескольких дней [1].

Основной раздел. Сервис обнаружения DDoS-атак представляет собой программный компонент, включающий в себя несколько подсистем:

- Подсистема настройки сервиса;
- Подсистема захвата сетевых пакетов;
- Подсистема математического анализа трафика;
- Подсистема анализа сетевых пакетов;
- Подсистема уведомлений.

Далее будет представлено подробное описание каждой подсистемы.

Подсистема настройки сервиса настраивает приложение путем считывания настроек из файла конфигурации. Подсистема следит за изменением настроек в этом файле, и если они изменены, то переконфигурирует приложение прямо во время его работы. Подсистема настройки управляет следующими атрибутами:

- список сетевых интерфейсов, с которых будет происходить захват трафика;
- максимальные пороги пакетов в секунду для фильтров анализа трафика;
- настройки уведомлений такие, как исходящий адрес электронной почты с логином и паролем, адрес SMTP-сервера и список электронных адресов, которым будут рассылаться уведомления об атаках;
- настройки расположения папок, в которых хранятся сетевые дампы и лог-файлы.

Подсистема захвата сетевых пакетов отвечает за прием сетевых пакетов и их передачу другим подсистемам. Подсистема может работать в многозадачном режиме, таким образом обслуживая несколько сетевых интерфейсов. Данная подсистема создает отдельный поток для каждого сетевого интерфейса. В этом потоке регистрируется слушатель захвата пакетов. Слушатель использует фильтр пакетов, чтобы принимать только входящий трафик, адресованный данному сетевому интерфейсу. Далее запускается цикл захвата пакетов. Принятые пакеты передаются в буфер пакетов, который используется анализаторами.

Подсистема математического анализа трафика собирает и хранит данные, которые передает подсистема захвата сетевых пакетов. Эти данные обрабатываются определенными математическими методами, которые, в свою очередь, дают представление об аномалиях входящего трафика [2]. Если подсистема математического анализа обнаружила атаку, то сразу же вступает в работу подсистема анализа сетевых пакетов.

Подсистема анализа сетевых пакетов проверяет заголовки входящих сетевых пакетов на предмет установки определенных флагов, используемых сетевыми протоколами, и подводит статистику их присутствия. Данная подсистема срабатывает только тогда, когда подсистема математического анализа обнаружила атаку. Подсистема принимает окончательное решение: была атака или нет. Чтобы выяснить причину возникновения аномалий во входящем сетевом трафике и извлечь подробную информацию об атаке, если та имела место, подсистема использует буфер сетевых пакетов. Буфер хранит сетевые пакеты, захваченные за определенный промежуток времени. Информация об атаке извлекается из заголовков сетевых пакетов. По заголовкам подсистема может определить три наиболее распространенных типа DDoS-атак на втором и третьем уровнях модели OSI:

– ICMP-flood – один из самых опасных видов DDoS-атак, использующий ICMP-сообщения для перегрузки сетевого канала атакуемого. У компьютера-жертвы после такой атаки произойдет отказ в обслуживании практически со стопроцентной вероятностью. Протокол межсетевых управляющих сообщений (ICMP) используется в первую очередь для передачи сообщений об ошибках и не используется для передачи данных. ICMP-пакеты могут сопровождать TCP-пакеты при соединении с сервером;

– UDP-flood – является аналогом ICMP-flood, где вместо ICMP-пакетов используются UDP-пакеты. Эта атака использует бессеансовый режим протокола UDP и заключается в отправке множества UDP-пакетов (как правило, большого объема) на определенные или случайные номера портов удаленного компьютера, который для каждого полученного пакета должен определить соответствующее приложение, убедиться в отсутствии его активности и отправить ответное ICMP-сообщение «адресат недоступен». В итоге атакуемая система окажется перегруженной: в протоколе UDP механизм предотвращения перегрузок отсутствует, поэтому после начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания, и полезному трафику останется лишь малая ее часть;

– TCP-SYN-flood – заключается в отправке большого количества TCP-пакетов с установленным флагом SYN в достаточно короткий срок. Согласно процессу «трехкратного рукопожатия» TCP, клиент посылает TCP-пакет с установленным флагом SYN (synchronize). В ответ на него сервер должен послать клиенту TCP-пакет с установленными флагами SYN и ACK (acknowledges). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным. Принцип атаки заключается в том, что злоумышленник, посылая TCP-пакеты с установленным флагом SYN, переполняет на сервере очередь на подключения. При этом он подделывает заголовок пакета таким образом, что ответный TCP-пакет с установленными флагами SYN и 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 подключений заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают ее с существенными задержками.

Подсистема уведомлений рассылает по электронной почте и через мессенджеры, такие как Telegram, Viber, WhatsApp, письма с сообщением об атаке и сохраняет сетевой дамп, который можно просмотреть с помощью Wireshark [3]. Подсистема срабатывает только тогда, когда подсистема анализа пакетов подтвердила атаку. Важно понимать, что проектируемая система не защищает от DDoS-атак, а только обнаруживает и уведомляет о них администраторов безопасности или других специалистов.

Предполагается, что управление сервисом будет производиться сторонним программным обеспечением, которое не будет рассматриваться в рамках данной статьи.

Заключение. В результате проектирования предлагается разработать сервис обнаружения сетевых атак. Сервис может работать с несколькими сетевыми интерфейсами одновременно. С каждого сетевого интерфейса происходит захват входящих сетевых пакетов. Захваченные пакеты интерпретируются как отсчеты дискретного сигнала или временного ряда. Временной ряд подвергается какому-любо математическому методу, который определяет присутствие аномалий, т.е. сетевых атак. Если с помощью математического анализа удалось обнаружить атаку, то проводится анализ сетевых пакетов, которые были захвачены. Анализ захваченных пакетов подтверждает или отклоняет гипотезу присутствия атаки. С помощью анализа пакетов устанавливается конкретный тип атаки (если она имела место), сохраняется дамп сетевых пакетов и отправляются уведомления об атаке администраторам сети.

ЛИТЕРАТУРА

1. Шелухин, О.И. Обнаружение вторжений в компьютерные сети. Сетевые аномалии / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – Горячая линия – телеком, 2013. – 220 с.
2. Комар, М.П. Система анализа сетевого трафика для обнаружения компьютерных атак / М.П. Комар // Вестник Брестского государственного технического университета. Серия «Физика, математика, и информатика». – 2010. – № 5. – С. 14–16.
3. Wireshark User’s Guide // Wireshark [Электронный ресурс]. – Режим доступа: https://www.wireshark.org/docs/wsug_html_chunked/. – Дата доступа: 20.09.2019.