Анализ трафика как инструмент исследования вычислительной сети

Д.В. Игнатов, e-mail: gato.blanco75@gmail.com
Д.Э. Назаренко, e-mail: gato.blanco75@gmail.com
М.В. Янов, e-mail: gato.blanco75@gmail.com

ВУНЦ ВВС «ВВА»

Аннотация. *Рассмотрены варианты использования анализа трафика в качестве инструмента исследования вычислительной сети и некоторые программные средства для его реализации.*

Ключевые слова: *локальная сеть, трафик, мониторинг, обнаружение вторжений.*

Введение

Анализ локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Под анализом понимается сложный и интеллектуальный процесс осмысления собранной информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети. Задача анализа требует активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов [1]. В то же время, вопрос выбора конкретных объектов для анализа сети и применяемых для этого инструментов является актуальным.

Выбор объектов и средств их анализа

Основным инструментом сбора данных о процессах, протекающих в локальной сети, является мониторинг.

Мониторинг сетевого трафика — непрерывный процесс инструментального автоматизированного наблюдения за отдельными параметрами трафика с целью проверки соблюдения SLA, планирования сети, а также предотвращения негативных событий, таких как технические аварии, угрозы и атаки злоумышленников [1].

Наиболее часто применяются следующие средства мониторинга [2]:

– анализаторы протоколов, или сетевые сниферы, позволяют захватывать трафик локальных сетей, представлять его в удобном для анализа виде, но собственно анализ данных оставляют администратору;

– маршрутизаторы, поддерживающие протокол NetFlow, собирают обобщенные данные о трафике глобальных сетей, передавая его для анализа программным системам NetFlow, которые автоматизируют поиск атак и угроз;

– системы обнаружения вторжений (Intrusion Detection Systems, IDS) специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей;

– системы контроля трафика и состояния сети административного назначения.

Анализаторы протоколов способны на основе некоторых заданных оператором логических условий захватывать отдельные пакеты и декодировать их, то есть показывать в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания полей каждого пакета. Анализатор протоколов представляет собой либо самостоятельное специализированное устройство, либо персональный компьютер, обычно переносной класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Анализатор протоколов подключается к сети точно так же, как обычный узел. Отличие состоит в том, что анализатор протоколов может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция — адресованные только ей. Программное обеспечение анализатора протоколов состоит из ядра, поддерживающего работу сетевого адаптера и декодирующего получаемые данные, и дополнительного программного кода, зависящего от типа исследуемой сети. В состав некоторых анализаторов может входить также экспертная система, способная выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправностей в сети. Основываясь на результатах анализа содержимого пакетов того или иного протокола, можно оптимизировать производительность сети, находить и устранять неполадки, осуществлять обоснованное и взвешенное изменение каких-либо компонентов сети. Обычно для того, чтобы сделать какие-либо выводы о влиянии некоторого изменения на сеть, анализ протоколов выполняется и до, и после внесения этого изменения [3]. Основным недостатком подобных систем является то, что они дают большой объем данных, которые достаточно сложно интерпретировать. Кроме того, данные

системы как правило адаптированы для разбора инцидентов, а не для анализа текущего состояния сети и абонентов.

Система мониторинга NetFlow собирает статистику не о каждом пакете, а о потоке пакетов, отсюда и название протокола (net — сеть, flow — поток). Под потоком понимается последовательность пакетов, принадлежащих одному и тому же соединению между определенными приложениями двух определенных компьютеров, например Skype-сеанс между двумя пользователями, передача файла с сервера на клиентский компьютер, чтение данных веб-страницы с сервера браузером клиентского компьютера. Аналогом потока можно считать данные телефонного разговора между двумя абонентами, однако между двумя компьютерами, в отличие от телефонов, может вестись сразу несколько «разговоров». Как правило, для анализа трафика используются наиболее характерные и значимые признаки:

– сетевые адреса источника и получателя;

– порты источника и получателя для основных транспортных протоколов, например UDP и TCP;

– тип и коды сообщения для служебных сообщений, например ICMP;

– номер интернет-протокола транспортного уровня, инкапсулированного в протокол сетевого уровня;

– тип обслуживания;

– используемый сетевой интерфейс и т.д.

Система NetFlow использует два основных программных компонента для своей работы. Компонент Экспортер потока (Flow Exporter) обеспечивает захват статистической информации о потоке и его передачу для дальнейшего анализа. Как правило, он настраивается на устройстве или узле, через который идет основной трафик, таком, как маршрутизатор или коммутатор. В случае высокой нагрузки или особых требований, допускается (и даже рекомендуется) установка нескольких экспортеров на одном устройстве для независимого перехвата потоков по различным критериям. Компонент Сборщик Потока (Flow Collector) обеспечивает функцию сбора информации, предоставляемой Экспортерами потока, её анализ, представление приложениям более высокого уровня получает данные о потоках и сохраняет их. Во многих современных решениях для анализа сетевого трафика функции коллектора и анализатора совмещают в едином программно-аппаратном блоке [3]. Достоинством подобных систем является то, что они обеспечивают удобную форму представления данных для анализа сетевого трафика, а также позволяют проводить как динамический анализ, так и детальный статистический разбор ситуаций с

сопоставлением в течение длительных промежутков времени. В то же самое время, данные системы обеспечивают ограниченные возможности по оперативному выявлению сетевых атак, так как не предполагают непосредственно анализ передаваемой информации: выявление атак производится в основном по признаку возникновения аномалий.

Система обнаружения вторжений (Intrusion Detection System, IDS) — это программное или аппаратное средство, которое выполняет непрерывное наблюдение за сетевым трафиком и деятельностью субъектов системы с целью предупреждения, выявления и протоколирования атак. В отличие от файерволов и прокси-серверов, которые строят защиту сети исключительно на основе анализа сетевого трафика, системы обнаружения вторжений учитывают в своей работе различные подозрительные события, происходящие в системе. Подобные системы могут иметь различные варианты реализации:

– сетевые системы анализа вторжений, размещаемые на границе вычислительных сетей и обеспечивающие обнаружение и противодействие атакам на маршрутизирующее оборудование;

– сетевые системы анализа вторжений локальных сетей, обнаруживающие характерные признаки атак, реализуемых в замкнутой сети (домене коллизий);

– сетевые системы анализа трафика протоколов, обеспечивающие обнаружение отдельных категорий атак, направленных на специфические протоколы и приложения (например, на обнаружение SQL-инъекций);

– системы обнаружения вторжений на основе анализа аномалий поведения сетевых служб и устройств (например, выявление атак доступа на сервера).

Основным недостатком с точки зрения использования в качестве инструмента анализа трафика является то, что большинство систем обнаружения вторжения имеют ограниченные возможности обмена информацией с внешними по отношению к ним пользовательскими приложениями, а также то, что они, как правило, используют заранее подготовленный набор сценариев для реакции на изменения сетевой обстановки.

– К последней категории средств можно отнести программные средства для контроля и управления сетями. Они представляют собой программные пакеты, позволяющие с использованием стандартных или специфических для определенного производителя протоколов осуществлять сбор данных о сетевых устройствах, их настройках, степени нагрузки, текущем трафике и отдельных его параметрах. Наиболее часто встречаются решения на основе использования

протоколов SNMP различных версий, а также технологии RMON. Последняя включает в себя отдельные компоненты, используемые для анализа трпафика:

– Statistics - совокупный сетевой трафик и статистика ошибок.

– Hosts – предоставление в табличном формате статистики по трафику для каждого сетевого узла, базируясь на его MAC-адресе;

– HostTopN - расширяет предыдущую группу, сортируя узлы, генерирующие максимальный трафик и число ошибок.

– Matrix - производит отслеживание величины трафика или количества ошибок между двумя устройствами в соответствии с их MAC-адресами;

– Filter - совместно с группой Packet Capture обеспечивает захват пакетов для последующего анализа.;

Данные системы обладают преимуществом высокой степени адаптированности к оборудованию определенных производителей, что является одновременно и достоинством, и недостатком.

Заключение

В тексте статьи проведен предварительный анализ существующих категорий средств для мониторинга вычислительных сетей и их исследований. Необходимость использования каждой из категорий средств мониторинга необходимо обосновывать в каждом конкретном случае, в зависимости от перечня решаемых задач (анализ состояния сети, поиск аномалий, оптимизация сетевых процессов), параметров самой сети и имеющихся в наличии материальных и финансовых ресурсов.

Список литературы

1. Славнов К.В. Управление информационной безопасностью. Учебное пособие / Славнов К.В., Барсуков О.М, Игнатов Д.В., Воронеж: ООО «Ритм», 2019. – 380 с.

2. Олифер В., Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. /Олифер В.,Олифер Н. - СПб.: Питер, 2016. - 992 с.

3. Бирюков А.А. Информационная безопасность: защита и нападение/ Бирюков А.А. – 2-е изд. перераб., доп. – М.: ДМК Пресс, 2017 – 434 с.