Автоматизация процессов моделирования угроз на уровне сети

Юрий Черкас, *региональный директор Skybox Security в России и СНГ*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*

Моделирование и оценка опасности угроз достаточно давно применяются на практике во многих компаниях в качестве превентивного метода защиты. Они позволяют своевременно выявить слабые места и принять меры по устранению имеющихся недостатков системы безопасности. В этой статье попробуем разобраться, применим ли такой подход на сетевом уровне. Возможно ли автоматически создавать все сценарии реализации угроз на уровне сети и так же автоматически оценивать их опасность?

С одной стороны, есть информационные ресурсы (объекты защиты), в частности сервисы и приложения, функционирующие в различных средах: физические и виртуальные серверы, контейнерные среды, рабочие станции и т.д. С другой стороны, есть источник угрозы в лице хакеров, действующих в сети Интернет, – внешний нарушитель или в лице нелояльных сотрудников – внутренний нарушитель. И эти нарушители пытаются атаковать в сети сервисы и приложения доступными инструментами. При этом, разумеется, используются различные средства сетевой безопасности, например межсетевые экраны, предназначенные для блокирования возможных векторов атак. В этой статье мы, рассматривая сетевой уровень, ограничимся локальным и удаленным сетевым доступом потенциального нарушителя, исключая угрозы, связанные с физическим доступом злоумышленника к оборудованию компании.

Как проанализировать совокупность всех факторов и с какими сложностями придется при этом столкнуться? При оценке вектора атаки в нашей модели предлагаем рассмотреть следующие основные параметры:

- источник угрозы (нарушитель);
- защищаемые информационные ресурсы (приложения или сервисы);
- условия для реализации угроз – наличие уязвимости и наличие сетевого доступа.

В результате анализа векторов атак мы ожидаем получить понимание всех возможных сценариев реализации угрозы с учетом реальных настроек нашей сети и имеющихся в инфраструктуре уязвимостей, а также оценить опасность каждой такой угрозы.

Рассмотрим более подробно процесс определения параметров моделирования угроз, перечисленных выше. С нарушителями как потенциальными источниками угроз более-менее все очевидно. Как сказано выше, они могут быть либо внешними, либо внутренними, в зависимости от того, откуда осуществляется атака. Из систем инвентаризации и сканеров защищенности можно получить как сам перечень защищаемых информационных ресурсов, так и информацию об имеющихся в сети уязвимостях, что в нашем случае является одним из условий для реализации угрозы. А вот для анализа второго условия реализации атаки (наличие сетевого доступа) мы как минимум должны знать текущие настройки сети и правил доступа на межсетевых экранах. И вот тут начинают появляться различные сложности, которые далее рассмотрим более подробно.

Сложности моделирования угроз

Анализ настройки сложных распределенных сетей

Сеть является одним из важнейших элементов ИТ-инфраструктуры любой организации. В состав сети входит достаточно большое количество активного сетевого оборудования (маршрутизаторы, коммутаторы, балансировщики нагрузки и др.) и межсетевых экранов различных производителей. Не стоит забывать и про активное использование виртуальных сетевых устройств, особенно учитывая растущую популярность таких технологий, как Cisco ACI или VMware NSX/NSX-T.

Общее количество подобных устройств, включая виртуальные, может достигать сотен и даже тысяч. Общее количество правил фильтрации, списков контроля доступа и прочих настроек, связанных с обеспечением безопасности и контроля сетевого доступа к элементам инфраструктуры, также может измеряться десятками и сотнями тысяч. В нашей практике нередко встречаются случаи, когда общее количество правил доступа переваливает

за 100 тыс. строк. При этом встречаются случаи, когда только на одном межсетевом экране настроено более 100 тыс. правил и 3–4 тыс. виртуальных интерфейсов.

Не стоит забывать и о том, что настройки сети динамично меняются, запускаются новые сервисы, вводится микросегментация. При этом управление оборудованием, как правило, выполняется посредством ряда консолей и модулей разных производителей, что значительно усложняет получение единой наглядной картины эффективного действия правил доступа по всей сети. В этих условиях контроль и периодический пересмотр такого объема настроек и правил сетевого доступа – очень трудоемкая задача, поэтому выполнить ее вручную практически невозможно.

Как следствие, организации довольно часто просто не знают, как выглядит их сеть в текущий момент времени. Статичные схемы, красиво выполненные, например, в Visio, к сожалению, практически никогда не отражают действительность, и мы нередко сталкиваемся с тем, что такие схемы демонстрируют картину "как это было год назад". Бывало даже, что номера сетей, включая IP-адресацию, не соответствовали реальной ситуации.

Актуальные сведения об уязвимостях

С наличием уязвимостей тоже все не так очевидно. Безусловно, сканеры эффективно выявляют уязвимости различных компонентов ИТ-инфраструктуры, но проблема в том, что сканирования проводятся на периодической основе, а некоторые сегменты вообще не сканируются (например, из-за того, что они недоступны для сканера защищенности). В результате получается, что полная актуальная картина отсутствует. Предположим, последнее сканирование было проведено месяц назад, но ведь в течение этого времени устанавливались обновления и патчи, и это означает, что часть данных уязвимостей уже устранена, а условия для реализации угрозы отсутствуют. С другой стороны, в среднем в мире каждый месяц обнаруживается порядка 600–1200 новых различных уязвимостей, а значит мы можем не знать о новых появившихся угрозах до следующего сканирования. Таким образом, мы можем ошибочно посчитать, что условия для реализации угрозы существуют (так называемые ошибки первого рода, или false positive), или наоборот, мы можем не знать об их существовании (ошибки второго рода, или false negative) (рис. 1).

В результате получается, что если мы хотим выстроить динамический процесс оценки возможных сценариев реализации угроз на сетевом уровне, то для этого нам необходимо учитывать два условия, а именно:

1. Иметь четкое представление сети с учетом всех ее настроек для анализа наличия/отсутствия сетевого доступа.
2. Понимать актуальный перечень имеющихся уязвимостей.

Очевидно, что сделать анализ всех возможных сетевых маршрутов от всех нарушителей до всех уязвимостей – задача крайне трудоемкая и без средств автоматизации здесь не обойтись.

На сегодняшний день существует целый ряд продуктов, направленных на автоматизацию процесса моделирования угроз на уровне сети. Одним из лидирующих продуктов является решение Skybox Security, которое давно представлено на российском рынке безопасности. Ниже рассмотрим более подробно функциональные возможности этого решения.

Skybox – платформа автоматизации моделирования угроз

Платформа Skybox Security позволяет автоматизировать следующие основные функции:

- динамическое моделирование карты сети, а также анализ настроек сетевого оборудования и межсетевых экранов;
- создание актуальной обновляемой базы защищаемых информационных ресурсов и имеющихся на них уязвимостей;
- моделирование угроз и симуляция атак путем анализа доступов от всех потенциальных нарушителей до всех имеющихся уязвимостей на модели сети;
- автоматический расчет опасности угроз с помощью гибко настраиваемой скоринговой модели;
- формирование рекомендаций по снижению уровня угрозы.

Моделирование сети

Для службы информационной безопасности важно понимать, как устроена сеть и какой доступ в ней разрешен, а какой запрещен, но для этого нужно понимать все настройки сетеобразующих устройств, включая правила маршрутизации, NAT, правила доступа межсетевых экранов, маршрутизаторов и т.д. При этом важно не только видеть текущую картину, но и отслеживать все изменения в реальном масштабе времени. Для этого Skybox собирает и анализирует все конфигурации сетевого оборудования, включая виртуальные и облачные сетевые сегменты, а затем строит динамически обновляемую модель, которая в точности отражает реальную сеть. В случае изменений настроек или правил Skybox просто загрузит новую конфигурацию и пересчитает модель.

Такая модель позволяет автоматически и без влияния на реальную сеть проверить второе условие реализации атаки, а именно вычислить и визуализировать на карте сети возможные маршруты прохождения заданного типа трафика с демонстрацией разрешающих и запрещающих правил и настроек, задействованных для этих маршрутов.

Необходимо отметить, что построенная сетевая модель дает и ряд дополнительных возможностей, которые не имеют прямого отношения к определению вектора атаки. Так, например, анализ конфигураций и настроек позволяет:

1. Автоматически осуществлять проверку конфигураций сетевого оборудования на соответствие лучшим практи-

Организации довольно часто просто не знают, как выглядит их сеть в текущий момент времени. Статичные схемы, красиво выполненные, например, в Visio, к сожалению, практически никогда не отражают действительность, и мы нередко сталкиваемся с тем, что такие схемы демонстрируют картину "как это было год назад".

На сегодняшний день существует целый ряд продуктов, направленных на автоматизацию процесса моделирования угроз на уровне сети. Одним из лидирующих продуктов является решение Skybox Security, которое давно представлено на российском рынке безопасности.

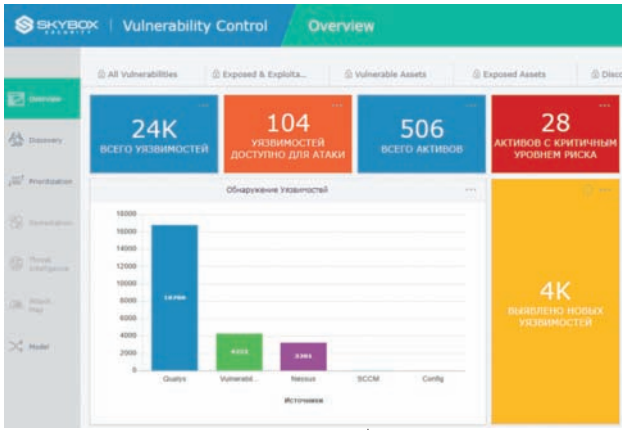

Рис. 1

Рис. 2

Настройка параметров нарушителя в Skybox полностью соответствует методике ФСТЭК России и фактически сводится к тому, чтобы указать расположение, тип нарушителя и его потенциал. При этом количество нарушителей может быть неограниченным.

кам и установленным в организации политикам конфигурирования.

2. Оптимизировать правила доступа межсетевых экранов:
- выявлять затененные и избыточные правила;
- выявлять редко используемые правила и объекты;
- формировать рекомендации по оптимизации правил и настроек.

3. Автоматически контролировать принятую политику сегментирования сети (доступ между зонами безопасности) с указанием причины несоответствия вплоть до конкретных правил на конкретных устройствах.

Skybox имеет собственную ежедневно обновляемую базу всех известных уязвимостей, а также информацию обо всех информационных ресурсах, включая данные об их версиях, установленных обновлениях и патчах. Используя встроенные алгоритмы, Skybox может автоматически проанализировать, для каких платформ, приложений и сервисов актуальны те или иные уязвимости.

Специализированные средства, такие как Skybox Security, позволяют не только моделировать все сценарии реализации угроз и автоматически оценивать их опасность, но и получить дополнительные возможности контроля конфигураций сетевого оборудования и политики сегментирования, анализа правил доступа межсетевых экранов и их изменений.

Моделирование нарушителей и анализ условий для реализации угроз

В ходе моделирования угроз и оценки их опасности нам также необходимо определить нарушителя, иметь перечень защищаемых информационных ресурсов и уязвимостей (второе условие для реализации угроз).

Настройка параметров нарушителя в Skybox полностью соответствует методике ФСТЭК России и фактически сводится к тому, чтобы указать расположение, тип нарушителя и его потенциал. При этом количество нарушителей может быть неограниченным.

С перечнем информационных ресурсов, в отношении которых рассматриваются угрозы, тоже все довольно просто. Skybox интегрируется с различными сканерами защищенности (например, MaxPatrol, Qualys, Tenable, Rapid7 и др.), а также с системами инвентаризации и патч-менеджмента (например, Microsoft WSUS и CSSM, Red Hat Satellite, IBM BigFix и др.). При этом существует возможность загрузки данных и из других источников с помощью встроенного Generic CMDB CSV Parser или API. Таким образом, Skybox позволяет не только сформировать полный список всех имеющихся информационных ресурсов, но и постоянно обновлять информацию об установленных версиях, обновлениях и патчах.

Важно отметить, что такая интеграция с различными системами позволяет не только получить список информационных ресурсов, но и иметь всегда полную и актуальную информацию об имеющихся уязвимостях даже в период "до" и "между" сканированиями, а также для сегментов, которые не сканируются по тем или иным причинам. Достигается это за счет использования встроенного движка "пассивного" выявления уязвимостей Vulnerability Detector. Работает этот движок следующим образом. Skybox имеет собственную ежедневно обновляемую базу всех известных уязвимостей, а также информацию обо всех информационных ресурсах, включая данные об их версиях, установленных обновлениях и патчах. Используя встроенные алгоритмы, Skybox может автоматически проанализировать, для каких платформ, приложений и сервисов актуальны те или иные уязвимости.

А далее Skybox приступает к выполнению самой трудоемкой задачи – анализу возможных маршрутов от всех нарушителей до всех имеющихся уязвимостей. Этот анализ как раз и позволяет проверить второе условие для реализации угрозы, а именно наличие сетевого доступа. Важный момент в том, что проверка именно этого условия позволяет отсеять колоссальное количество угроз и признать их неактуальными, так как при отсутствии сетевого доступа эксплуатация уязвимости не представляется возможной. При этом также производится автоматическая оценка опасности каждой актуальной угрозы, что позволяет сфокусироваться на устранении наиболее критичных векторов атак.

В итоге остается только определиться с тем, какой из предложенных Skybox вариантов снижения уровня угрозы выбрать. И это может быть не только устранение самой уязвимости путем установки обновлений или патчей, но и активация сигнатур системы предотвращения атак (IPS) или блокировка сетевого доступа по конкретным адресам или портам (рис. 2).

Таким образом, моделирование угроз на сетевом уровне можно практически полностью автоматизировать. Специализированные средства, такие как Skybox Security, позволяют не только моделировать все сценарии реализации угроз и автоматически оценивать их опасность, но и получить дополнительные возможности контроля конфигураций сетевого оборудования и политики сегментирования, анализа правил доступа межсетевых экранов и их изменений. При этом решения подобного класса востребованы не только службами информационной безопасности (с точки зрения повышения реального уровня защищенности), но и подразделениями ИТ, поскольку они позволяют получать актуальную информацию по карте сети в режиме реального времени. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru