Лекция 3
Сканеры сетевой безопасности

1. Сканер уязвимости сети
2. Механизмы работы сетевого сканера локальной сети
3. Возможности современных программных решений
4. Сравнение сканеров уязвимостей сети
5. Вопросы

Сканер уязвимости сети

Одним из важнейших этапов обеспечения информационной безопасности является идентификация потенциальных рисков. Большинство ИТ-специалистов знают, насколько может быть опасна «брешь» в ОС и приложениях. И чрезвычайно важно найти эти «дыры», или на языке профессионалов - уязвимости, прежде, чем ими смогут воспользоваться недоброжелатели. Для этой цели и были созданы сканеры безопасности.

Продвинутые специалисты по IT-безопасности используют в своей работе специализированное аппаратное или программное обеспечение, сканирующее сеть и ее устройства на предмет обнаружения слабых мест в системе безопасности. Это и есть сканеры уязвимости, или по-другому — безопасности, сети. Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. Грамотно используя сканер уязвимости сети, специалист может значительно усилить сетевую безопасность.

Сканер уязвимости сети — автоматизированное решение для проведения полного сканирование портов, контроля необходимых обновлений ПО для защиты сети, а также проверки программного и аппаратного обеспечения.

Таким образом, сетевые сканеры направлены на решение следующих задач:

- идентификация и анализ уязвимостей;
- инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;
- формирование отчетов, содержащих описание уязвимостей и варианты их устранения.

Сканер локальной сети — жизненно необходимое средство для компаний, чья деятельность напрямую связана с хранением и обработкой уникальных баз данных, конфиденциальной информации, ценных архивов. Без сомнения, сканеры сети необходимы организациям в сферах обороны, науки, медицины, торговли, IT, финансов, рекламы, производства, для органов власти и диспетчерских служб — словом, везде, где нежелательна или даже опасна утечка накопленной информации, имеются базы персональных данных клиентов.

Механизмы работы сетевого сканера локальной сети

Сканеры уязвимостей сети при своей работе используют два основных механизма. Первый — зондирование — не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. При зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы».

Второй механизм — сканирование — более быстрый, но дает менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения ее наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. Они в

дальнейшем сравниваются с таблицей правил определения сетевых устройств, ОС и возможных «дыр». После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимости.

В общем случае алгоритм работы сканеров следующий:

- Проверка заголовков. Самый простой и быстрый способ на основе сканирования, однако имеющий ряд недостатков. Так, вывод о «провале» делается лишь по результатам анализа заголовков. К примеру, проверяя FTP-сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Естественно, специалисты по сетевой безопасности осведомлены о ненадежности этого метода, однако как первый шаг сканирования — это оптимальное решение, не приводящее к нарушению работы сети.
- Активные зондирующие проверки (active probing check). Это сканирование, при котором не проверяется версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости. По тому же принципу действуют антивирусные программы, сравнивая ПО с имеющимися в базе сигнатурами вирусов. Тоже достаточно быстрый метод, хотя и медленнее первого, с большим коэффициентом надежности.
- Имитация атак (exploit check). Это зондирование, которое эксплуатирует дефекты в программном обеспечении. Таким образом подается своеобразный импульс некоторым уязвимостям, которые не заметны до определенного момента. Эффективный метод, однако применить его можно не всегда. Так, вероятна ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети или уязвимость окажется негодна для реализации атаки.

Большинство современных сканеров безопасности сети работает по нижеперечисленным принципам:

- сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;
- обнаружение потенциальных уязвимостей;
- подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки;
- формирование отчетов;
- автоматическое устранение уязвимостей. Не всегда данный этап реализуется в сетевых сканерах безопасности, но часто встречается в сканерах системных. Существует возможность создания резервного сценария, который может отменить произведенные изменения, — например, если после устранения уязвимости будет нарушено полноценное функционирование сети.

Тем не менее каждый сканер из множества представленных сейчас на рынке выделяется своими функциями и возможностями.

Возможности современных программных решений

Одним из главных требований к современным сетевым сканерам уязвимостей, помимо собственно безопасности, является поддержка различных операционных систем. Большинство популярных сканеров — кроссплатформенные (включая мобильные и виртуальные ОС).

Сканеры сети исследуют сразу несколько портов, что снижает время на проверку. И конечно, сканер должен проверить не только операционную систему, но и программное обеспечение, особое внимание уделяя популярным в хакерской среде продуктам Adobe Flash Player, Outlook, различным браузерам.

К полезной функции сканеров нужно отнести и проверку раздробленной сети, что избавляет администратора от необходимости оценивать каждый узел в отдельности и несколько раз задавать параметры сканирования.

Современные сканеры просты в использовании, их работу можно настроить в соответствии с потребностями сети. Например, они позволяют задать перечень

проверяемых устройств и типов уязвимостей, указать разрешенные для автоматического обновления приложения, установить периодичность проверки и предоставления отчетов. Получив подробный отчет об уязвимостях, одним нажатием кнопки можно задать их исправление.

Из дополнительных возможностей стоит выделить экономию трафика и анализ «исторических» данных. Так, скачивание лишь одной копии каждого дистрибутива и распределение этих копий по сети позволяет значительно снизить трафик. А сохраненная история нескольких сканирований позволяет оценить безопасность узла в определенном временном интервале, оптимально настроить работу программного и аппаратного обеспечения.

Сравнение сканеров уязвимостей сети

Российский рынок сканеров сейчас огромен, и каждый производитель пытается привлечь на свою сторону большую часть пользователей, обещая широкие возможности при низких ценах. К сожалению, далеко не все ожидания оправдываются. Разберем сильные и слабые стороны сетевых сканеров, возглавляющих экспертные рейтинги.

GFI LanGuard

Одна из компаний-лидеров на рынке информационной безопасности — GFI Software. Компания работает с 1992 года и за это время заслужила репутацию надежной организации, производящей профессиональные продукты для решения широкого спектра ИТ-задач.

GFI LanGuard — программное средство, обеспечивающее централизованную проверку на уязвимости во всей сети. Достоинство сканера в том, что, помимо обнаружения открытых портов, небезопасных настроек и запрещенного к установке ПО, он проверяет обновления и патчи не только ОС (десктопных и мобильных, физических и виртуальных), но и установленного ПО. Сканер уязвимости проверяет все: от серверов до сетевого аппаратного обеспечения, от виртуальных машин до смартфонов.

Закончив сканирование, GFI LanGuard отправляет пользователю полный отчет с характеристиками всех уязвимостей и инструкциями по их ликвидации в ручном режиме. Дружелюбный интерфейс позволяет сразу же закрыть «провал» в защите, исправить настройки, обновить ПО (включая установку недостающих элементов), «снести» запрещенные программы. Сканер сетевой безопасности можно настроить на полностью автономный режим работы, в этом случае он будет запускаться по таймеру, а исправления, разрешенные администратором, будут выполняться автоматически.

Данный сканер уязвимостей сети имеет очень важное отличие от множества конкурентов. Он может автоматически обновлять устаревшее программное обеспечение и устанавливать обновления и патчи на разные операционные системы.

Множество ИТ-специалистов в России выбирают именно GFI LanGuard: не случайно он занимает верхние строчки в рейтингах сетевых сканеров.

Стоимость владения лицензией GFI LanGuard обойдется от 900 рублей на один узел в год. Цена вполне доступна даже для небольшой организации, особенно учитывая, сколько трудовых ресурсов экономит сетевой сканер безопасности.

Nessus

Проект был запущен еще в 1998 году, а в 2003 разработчик Tenable Network Security сделал сетевой сканер безопасности коммерческим. Но популярность продукта не упала. Согласно статистике более 17% пользователей предпочитают именно Nessus. Регулярно обновляемая база уязвимостей, простота в установке и использовании, высокий уровень точности — его преимущества перед конкурентами. А ключевой особенностью является использование плагинов. То есть любой тест на проникновение не зашивается наглухо внутрь программы, а оформляется в виде подключаемого плагина. Аддоны распределяются на 42 различных типа: чтобы провести пентест, можно активировать как отдельные плагины, так и все плагины определенного типа — например, для выполнения

всех локальных проверок на Ubuntu-системе. Интересный момент — пользователи смогут написать собственные тесты с помощью специального скриптового языка.

Количество загрузок (а их уже более пяти миллионов) говорит за все отзывы. Nessus — отличный сканер уязвимостей сетей. Но есть у него и два недостатка. Первый — при отключенной опции «safe checks» некоторые тесты на уязвимости могут привести к нарушениям в работе сканируемых систем. Второй — цена. Годовая лицензия может вам обойтись в 114 тысяч рублей.

Symantec Security Check

Бесплатный сканер одноименного производителя. Основные функции — обнаружение вирусов и троянов, интернет-червей, вредоносных программ, поиск уязвимостей в локальной сети. Это онлайн-продукт, состоящий из двух частей: Security Scan, которая проверяет безопасность системы, и Virus Detection, выполняющей полную проверку компьютера на вирусы. Устанавливается быстро и просто, работает через браузер. К сожалению, по итогам многих тестов уступает большинству конкурентов, хотя все свои основные функции выполняет. Согласно последним отзывам, этот сканер сети лучше использовать для дополнительной проверки.

XSpider

Компания Positive Technologies работает на рынке более 10-ти лет и обладает одним из крупнейших исследовательских центров безопасности. У этой корпорации тоже есть свой сетевой сканер — программа XSpider, которая, по заявлению разработчика, может выявить треть уязвимостей завтрашнего дня. Ключевой особенностью этого сканера является возможность обнаружения максимального количества «провалов» в сети еще до того, как их увидят хакеры. При этом сканер работает удаленно, не требуя установки дополнительного ПО. Отработав, сканер отправляет специалисту по безопасности полный отчет и советы по устранению «дыр».

Отдельно отметим систему обновления программных модулей и базы уязвимостей, функции одновременного сканирования большого числа рабочих станций и сетевых узлов, ведение полной истории проверок, встроенную документацию и механизм генерации детализированных отчетов. Также стоит отметить, что XSpider сертифицирован Минобороны и ФСТЭК России.

Стоимость лицензии на этот сканер начинается от 11 тысяч рублей на четыре хоста в год.

QualysGuard

Многофункциональный сканер уязвимостей. Он предоставляет обширные отчеты, которые включают:

- оценку уровня критичности уязвимостей;
- оценку времени, необходимого для их устранения;
- проверку степени их воздействия на бизнес;
- анализ тенденций в области проблем безопасности.

Фирма-разработчик продукта, Qualys, Inc., широко известна в мировой среде ИТ-специалистов, у которых этот сканер пользуется доверием. Достаточно сказать, что около 50-ти компаний из списка Forbes «Global 100» используют данный продукт.

Облачная платформа QualysGuard и встроенный набор приложений позволяют предприятиям упростить процесс обеспечения безопасности и снизить затраты на соответствие различным требованиям, при этом предоставляя важную информацию о безопасности и автоматизируя весь спектр задач аудита, комплекс-контроля и защиту ИТ-систем и веб-приложений. С помощью данного ПО можно сканировать корпоративные веб-сайты и получать автоматизированное оповещение и отчеты для своевременного выявления и устранения угроз.

Итак, при выборе сетевого сканера безопасности учитывайте перечень его возможностей, но не забывайте соизмерять функционал продукта с потребностями своей организации и ее материальными возможностями. Основное, что нужно в работе сканера,

— широкий охват сети проверяемых устройств и узлов, простота в использовании и точность настроек, возможность автоматической работы, которая не будет отвлекать специалистов от повседневных задач.

Вопросы

1. Охарактеризуйте сканеры безопасности сети.
2. На решение каких задач направлены сетевые сканеры?
3. Опишите основные механизмы работы сканеров уязвимости сетей.
4. Опишите общий алгоритм работы сканеров.
5. По каким принципам работает большинство современных сканеров безопасности сети? Перечислите их.
6. Перечислите основные функции сетевых сканеров.
7. Опишите любой конкретный программный продукт (любой сетевой сканер безопасности).