УДК 004.49

В.В. Герман

ПРИМЕНЕНИЕ СКАНЕРОВ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Рассматриваются проблемы, возникающие при проведении аудита безопасности компьютерной сети с использованием сканеров безопасности. В первой части статьи приведены результаты исследований, которые позволили автору предложить классификацию современных сканеров безопасности. Предложенная классификация в значительной степени способствует формированию грамотного понимания специфических особенностей данных средств анализа защищенности и помогает ориентироваться в теме не только специалистам, но и неподготовленному читателю. Вторая часть работы посвящена проблемам, связанным с применением сканеров безопасности. В заключительной части статьи предложены практические рекомендации, направленные на повышение степени достоверности отчетов, полученных в результате их тестирования.

Уровень защищенности компьютерных систем от угроз безопасности зависит от многих факторов. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного программного обеспечения (ПО), средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты информационной системы (ИС) имеют сотни параметров, значения которых влияют на защищенность системы, что делает их анализ трудновыполнимой задачей.

Поэтому в современных ИС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации обычно используются специализированные программные средства.

Сканеры безопасности являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Современные сканеры безопасности можно условно классифицировать по следующим признакам (рисунок 1):

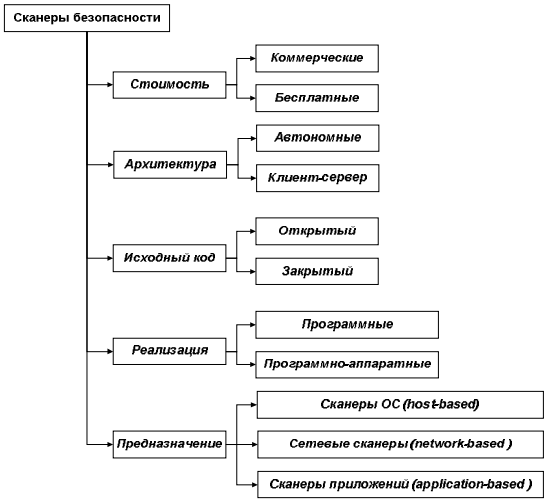

Рисунок 1 – Классификация сканеров безопасности.

1) <u>по стоимости</u>:

– бесплатные – распространяемые свободно, без ограничений на количество тестируемых узлов;

– коммерческие – стоимость лицензий на такие сканеры безопасности может варьироваться от сотни до нескольких сотен тысяч долларов;

2) <u>по архитектуре</u>:

– автономные сканеры безопасности – представляют собой самостоятельное программное обеспечение. Сканирующие модули и база данных уязвимостей входят в дистрибутив ПО и хранятся локально на персональном компьютере;

– клиент-сервер – в дистрибутив входят клиентская и серверная части. Прикладная программа или конечный пользователь взаимодействуют с клиентской частью системы, которая в простейшем случае обеспечивает просто надсетевой интерфейс. Клиентская часть системы при потребности обращается по сети к серверной части. Интерфейс серверной части определен и фиксирован;

3) <u>по исходному коду:</u>

– исходный код открыт – пользователь имеет возможность оценить грамотность реализации сканирующих модулей и при необходимости внести свои изменения;

– исходный код закрыт – как правило, такая ситуация характерна для коммерческих продуктов. Легальный пользователь лишен возможности ознакомления и модификации исходного кода сканера безопасности;

4) <u>по реализации:</u>

– программные;

– программно-аппаратные;

5) <u>по предназначению</u>:

– сканеры ОС – анализируют в первую очередь параметры, характерные для всего семейства одной ОС: шаблоны настроек, поиск известных уязвимостей и т.д.;

– сетевые сканеры – это программы для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей. Помимо обычного сканирования они различными средствами определяют версии ПО и проверяют по своей базе наличие известных уязвимостей и в случае их нахождения дают краткое описание и руководство к их устранению. Также выдается информация о степени опасности данной уязвимости. К сетевым сканерам относятся: ***сканеры портов*** **(**поиск открытых *TCP* и *UDP* портов) и ***CGI сканеры*** (сканируют *WEB* сервера на наличие уязвимых скриптов, директорий или ошибок *WEB* серверов);

– сканеры приложений – ориентированы на конкретные прикладные системы типа СУБД (*Microsoft SQL Server, Sybase Adaptive Server), Web-броузеров (Microsoft Internet Explorer, Netscape Navigator)* и т.п.

Практика применения сканеров безопасности для анализа защищенности ИС позволяет сформулировать ряд проблем, которые могут в значительной степени повлиять на достоверность результатов тестирования.

Приведем лишь некоторые из них.

1. Ложные срабатывания сканеров безопасности – могут быть следствием:

– ошибок в реализации сканирующих модулей;

– сбоев в системе электропитания, неисправности оборудования в момент тестирования;

– особенностей конфигурации конкретной ИС;

при пассивном анализе:

– информация о версии ПО, указываемая в заголовке ответа на запрос, не всегда говорит о его уязвимости;

– в целях противодействия сбору информации о ИС текст заголовка (информация о версии ОС, ПО) был предварительно изменен.

2. Отсутствие уязвимости в отчете – не может гарантировать защищенность ИС и может быть следствием:

– устаревших баз данных сканера безопасности;

– возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы (например, при удаленном тестировании узла, подсистема защиты может блокировать попытки сканера безопасности получить доступ к реестру ОС).

3. Нарушение работоспособности ИС – некорректное использование функциональных возможностей сканеров безопасности может привести не только к искажению результатов тестирования, но и отразиться на функциональных возможностях тестируемой ИС или полностью вывести ее из строя.

4. Сложность тестирования больших территориально-распределенных систем – эффективное применение сканеров безопасности, в данном случае может осложняться повышенными требованиями к пропускной способности используемых каналов связи, коммутирующего оборудования и т.д.

Приведем практические рекомендации, которые могут помочь решить обозначенные проблемы.

– Противодействие “ложным срабатываниям” – некоторые сканеры безопасности (SecPoint) имеют собственные встроенные механизмы противодействия “ложным срабатываниям”. Однако корректность реализации данных механизмов не является очевидной. Поэтому основной рекомендацией в данном случае может быть повторное тестирование с применением других сканеров безопасности и последующий сравнительный анализ результатов.

– Регулярное обновление сканера безопасности и его баз данных уязвимостей – недостаточное внимание к данной задаче может привести к появлению чувства “ложной защищенности”. Поэтому важно отслеживать последние обновления и исправления используемых сканеров безопасности. Большинство современных сканеров позволяют производить обновления версий сканеров безопасности и их баз данных в автоматическом режиме через сеть Интернет. Несмотря на это, необходимо контролировать этот процесс, поскольку нарушение целостности ПО может привести к возникновению новых проблем.

– Отказ от “шаблонного” тестирования – сканеры безопасности, как правило, обладают готовыми шаблонами для тестирования системы защиты. Вместе с тем аналитик, использующий сканер безопасности, должен самостоятельно определять именно те уязвимости, которые являются критичными для конкретной системы. Пренебрежение этим фактом может не только снизить функциональные возможности тестируемой системы, но и полностью вывести ее из строя.

Именно поэтому крайне важно до проведения тестирования проанализировать конкретную систему: состав оборудования, функциональное предназначение, особенности архитектуры и т.д.

В зависимости от ситуации тестирование может быть различным. Так, например, не рекомендуется производить сканирование сетевых узлов на наличие всех известных уязвимостей в ходе одного теста. Поскольку это может привести к "засорению" сетевого трафика и значительно снизить общую скорость. Поэтому сканирование лучше осуществлять поэтапно. Для некоторых ИС подобные условия могут оказаться неприемлемыми – в этом случае тестирование может осуществляться во вне рабочее время.

– Применение распределенного сканирования – при анализе защищенности больших территориально-распределенных ИС задача может быть решена путем независимого тестирования каждой из подсистем в отдельности.

– Применение многоуровневого сканирования – позволяет получить более полную картину о степени защищенности ИС и тем самым значительно повысить достоверность результатов тестирования. Так, сканирование на уровне ОС позволяет имитировать действия злоумышленника, имеющего непосредственный доступ к низкоуровневым возможностям хоста, конкретным сервисам и деталям конфигурации. Тогда как сканер сетевого уровня имитирует действия внешнего нарушителя системы безопасности.

В заключение хотелось бы еще раз подчеркнуть, что, несмотря на многочисленные преимущества, предоставляемые сканерами безопасности, необходимо учитывать массу факторов, которые в значительной степени могут повлиять на корректность результатов тестирования системы защиты информации.

Ни один из существующих на данный момент сканеров безопасности не позволяет в полной мере решить задачу оценки уровня защищенности ИС.

Поэтому для получения наиболее достоверных данных рекомендуется:

– для проведения анализа защищенности не ограничиваться только одним сканером безопасности;

– для оценки эффективности мер противодействия обнаруженным в системе уязвимостям и отслеживания динамики их появления рекомендуется производить периодическое тестирование системы защиты.

Библиографический список

1. *Никсов Д., Рудель П.* Сравнительный анализ сканеров безопасности. Часть 1. Использование сканеров безопасности в процессе тестирования сети на устойчивость к взлому - М.: Информзащита, 2005.