XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.82-83

УДК 004.7

Е.А.Кикинзон (5 курс, каф. АиВТ), В.М.Ицыксон, к.т.н., доц.

РАЗРАБОТКА ВИЗУАЛЬНОГО КОНФИГУРАТОРА ДИНАМИЧЕСКИХ СЕТЕВЫХ ЭКРАНОВ

Задача обеспечения безопасности локальных сетей и отдельных компьютеров, подключённых к глобальным сетям, продолжает оставаться достаточно актуальной на протяжении многих лет. Защита от несанкционированного доступа извне из проблемы крупных организаций постепенно перерастает в заботу пользователя каждого персонального компьютера, имеющего постоянное соединение с Internet. На сегодняшний день сколь угодно удалённый злоумышленник представляет серьёзную угрозу как для сохранности данных, так и для работоспособности системы в целом. Таким образом, возникает необходимость в относительно простых и дешёвых средствах защиты от внешней угрозы, которые будут доступны не только корпорациям, для которых безопасность внутренних сетей является жизненно важной, но и отдельным пользователям, не желающим становиться жертвами случайных атак.

Одним из наиболее распространённых решений в данной области являются сетевые фильтры, позволяющие контролировать прохождение пакетов и запрещать обращения к наиболее уязвимым сетевым сервисам. Поэтому неудивительно, что базовые средства фильтрации пакетов включаются в состав операционных систем, изначально ориентированный на работу в сети – здесь в первую очередь речь идёт о семействе операционных систем *nix. Тем не менее, все они предполагают управление встроенным сетевым фильтром посредством команд, записанных в файле сценария, что делает нетривиальную задачу конфигурирования брандмауэра ещё более сложной и трудоёмкой. Исходя из этого, можно сделать вывод об актуальности программных средств, позволяющих скрыть от пользователя конкретный формат команд и предоставляющих возможность оперировать с укрупнёнными сетевыми объектами.

Файлы сценариев, содержащие команды конфигурирования сетевого фильтра, могут иметь размер в несколько тысяч строк, причём многие из них будут отличаться весьма незначительно. Это объясняется тем, что системные средства предполагают указание конкретного IP-адреса или их диапазона, а также, при необходимости, и определённого номера порта для каждого правила. Таким образом, взаимодействие более крупных объектов, таких как локальные сети и их группы, должно быть разбито на более конкретные и узкие описания, что порождает практически идентичные команды, зачастую отличающиеся лишь одним аргументом. Подобный подход увеличивает число синтаксических и логических ошибок, а также делает непонятным функционирование достаточно сложной системы. Особенно актуальной становится данная проблема при необходимости внести некоторые изменения в существующий набор правил, т.к. подобная операция оказывается чрезмерно затруднённой.

Исходя из описанных особенностей системных средств, был определён набор функций, реализуемых дополнительным программным обеспечением, облегчающим настройку сетевого фильтра. Пользователю должны предоставляться возможности по описанию сетевых объектов и их групп, заданию поведенческих правил взаимодействия между ними, а также удобный графический интерфейс, позволяющий осуществлять данные операции. Кроме этого, среди актуальных задач стоит отметить и динамическое управление сетевым фильтром, позволяющее однократно задать расписание для определённых правил на стадии

описания сетевого фильтра, тогда как изменение конфигурации будет осуществляться автоматически в указанным моменты времени.

Для реализации данных задач разумно выделить совокупность объектов, содержащих описание различных сетевых узлов, служб и предоставляющих основные методы для внесения и модификации этой информации, а также набор функций, осуществляющих выделение и группирование необходимой информации в соответствии с правилами, описанными пользователем. Благодаря этому удастся избежать дублирования данных о сетевых объектах и обеспечить удобство их редактирования, гарантирующее обновление всех уже существующих правил, в которых эти объекты фигурируют. Таким образом, пользователю достаточно однократно описать те сетевые узлы и службы, взаимодействие между которыми он считает необходимым контролировать, а затем при помощи интерфейса осуществлять необходимое группирование и определение реакции сетевого фильтра.

В качестве решения задачи динамического управления пользователю предоставляется возможность описывать определённые интервалы времени и ставить их в соответствие правилам, имеющим ограниченный срок действия. Программное обеспечение в случае использования динамических правил создаст совокупность файлов сценариев и расписание для системного демона, определяющее последовательность запуска данных файлов. В случае, если динамические правила не используются, файл сценария будет единственным. Данный подход позволяет реализовать поставленную задачу без использования дополнительных резидентных программ, занимающих память и снижающих производительность системы.

В заключение хотелось бы отметить, что описанное программное обеспечение позволяет существенно упростить администрирование небольших локальных сетей, обеспечивая не только снижение трудоёмкости на этапе разработки сетевых фильтров, но и значительное облегчение их дальнейшего изменения и сопровождения.