УДК 004.771

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ЛОКАЛЬНЫХ СЕТЕЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Волковский С.О.
Днепропетровский национальный университет им. О. Гончара
Факультет физики, электроники и компьютерных систем
Кафедра ЭВМ

Аннотация

Волковский С.О. Обеспечение защиты локальной сети от несанкционированного доступа. *В статье рассматриваются вопросы использования в качестве комбинированного средства защиты локальной сети от несанкционированного доступа возможностей ОС семейства Linux.*

Общая постановка проблемы. Каждая компания, состоящая более чем из одного сотрудника, использующего для работы компьютер, нуждается в создании сети, объединяющей рабочие станции своих сотрудников. Грамотная организация сети, включающая организацию доступа в глобальную сеть (интернет), является составляющей продуктивности работы компании. При этом сеть, объединяющая информацию на компьютерах сотрудников компании, нуждается в защите, т.к. несанкционированное проникновение в сеть влечет за собой утечку информации или вообще может привести к выходу сети из рабочего состояния.

Постановка задач исследования. На сегодняшний день существует множество решений по защите компьютерных систем от внешнего проникновения, рассчитанных на различные условия использования и обеспечивающих различные степени защиты. Целью данной работы было исследование существующих продуктов и создание комбинированного средства защиты, отличающегося простотой установки и настройки, а также обеспечивающего достаточный уровень зашиты для противодействия большинству известных видов сетевых атак. Одним из требований к создаваемой системе является также возможность ее модульного расширения, что позволяет обеспечить динамическое конфигурирование согласно условиям конкретной системы. Создаваемая система должна быть бесплатной и базироваться на условиях распространения продуктов с открытым исходным кодом по лицензии GPL v3.

Решение задачи и результаты исследований. Для решения поставленной задачи был проведен анализ существующих программных продуктов, удовлетворяющих перечисленным требованиям. В качестве платформы была выбрана система Ubuntu Linux версии 9.10, что делает комплекс совместимым со всеми операционными системами семейства Linux, построенными на ядре версии не ниже 2.6.17. Для реализации системы защиты была выбрана схема с предварительным пакетным фильтром, работающим на уровне ядра операционной системы и сетевом уровне модели OSI. Данный модуль обеспечивает низкоуровневую фильтрацию пакетов по IP и TCP заголовкам и на основе анализа структуры пакетов. Этот способ позволяет защитить целевой хост от сканирования портов, а также от некоторых видов сетевых атак, направленных на переполнение буфера.

Для реализации системы защиты использован межсетевой экран Netfilter, являющийся частью операционных систем семейства Linux, построенных на ядре версий 2.4 и 2.6. Netfilter представляет собой систему маршрутизации входящих и выходящих пакетов с возможностью их обработки и фильтрации. Данный брандмауэр работает по принципу прохождения пакетом нескольких цепочек маршрутизации, каждая из которых состоит из правил маршрутизации. Каждая цепочка представляет определенную стадию пути пакета от

сетевого интерфейса до локального приложения и в обратную сторону – от приложения до сетевого интерфейса. Оригинальный модуль, реализующий фильтрацию пакетов, использует возможность системы Netfilter добавления правил маршрутизации для каждой цепочки прохождения пакета. Всего существует пять типов цепочек, встроенных в систему:

- PREROUTING – для всех пакетов, принятых на сетевой интерфейс.
- INPUT – для пакетов, перенаправленных запросившему их локальному приложению.
- FORWARD – для входящих пакетов, транслируемых на выход сетевого интерфейса без участия локальных процессов.
- OUTPUT – для пакетов, исходящих от локальных приложений.
- POSTROUTING – для обработки пакетов перед передачей в сеть.

Разрабатываемый пакетный фильтр использует задание правил в цепочках PREROUTING, осуществляя анализ заголовков всех входящих пакетов и OUTPUT в целях мониторинга исходящих запросов на соединение, что является частью защиты от SYN и ACK сканирования портов.

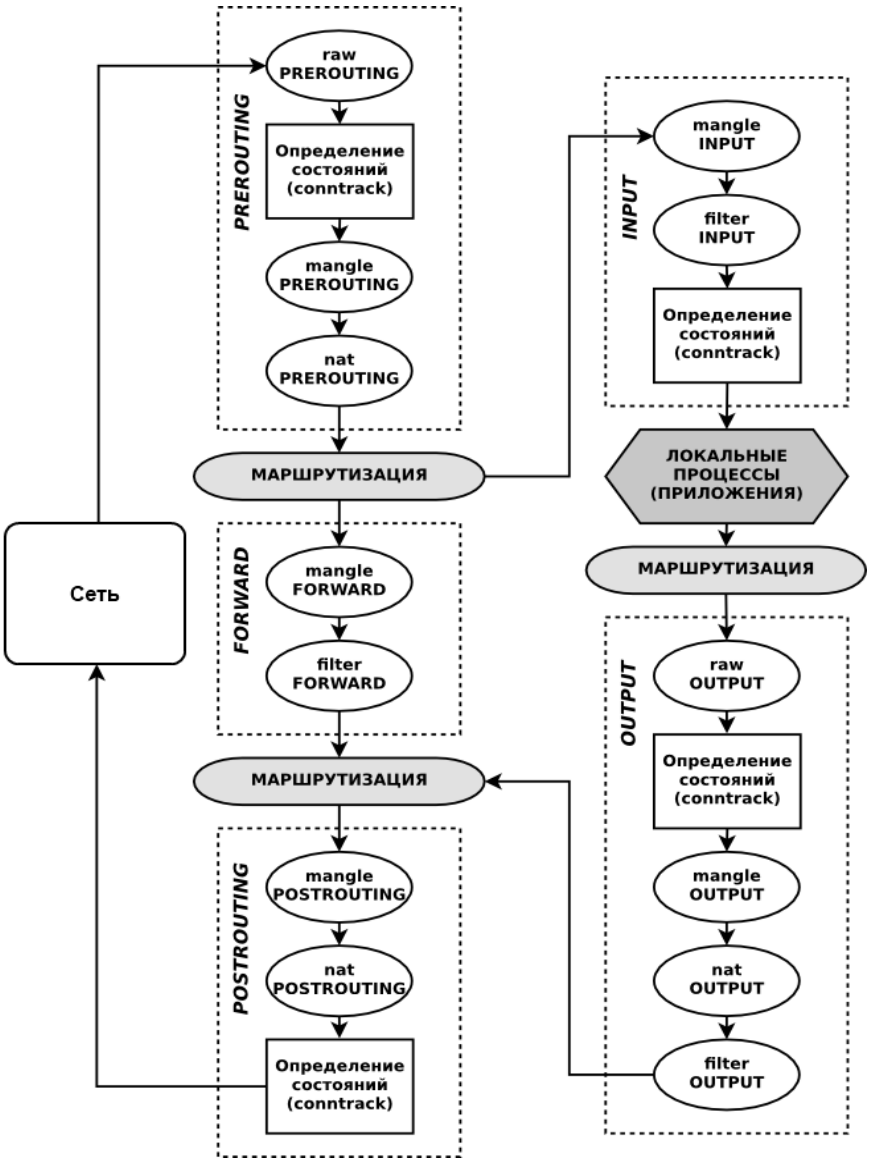

Рис.1 схема прохождения пакетов по цепочкам Netfilter

Пакеты, прошедшие низкоуровневый фильтр перенаправляются далее на прикладной уровень, где производится их анализ на наличие потенциально опасного для сети

пользователя программного кода, инкапсулированного во входящие данные. Для корректного анализа входящих данных используется модуль Layer 7 packet classifier, являющийся дополнением к Netfilter. Данное средство позволяет распознавать пакеты различных сетевых протоколов (HTTP, FTP, SNMP, SSH и т.д.) независимо от номера порта, на который пакет поступил. Исходя из дифференциации данных по протоколам, задействуются соответствующие модули эвристического анализа, что предоставляет возможность эффективного распознавания специфичных для каждого протокола приемов получения несанкционированного доступа к пользовательской сети.

В общем виде схема работы системы защиты сводится к фильтрации пакетов на сетевом уровне через изолированную область памяти с удалением пакетов, содержащих потенциально опасные включения.

Определяющими факторами алгоритма работы пакетного фильтра являются:

- количество потоков входящего и исходящего трафика, зависящее от количества сетевых интерфейсов.
- схема маршрутизации трафика, которая не должна быть нарушена при работе системы защиты.

Последующие действия с входными данными предполагают фильтрацию на уровне приложений по прокси-серверной схеме

При этом опасность исполняемого кода, возможно включенного в данные, определяется на основе доверительных интервалов для конкретного уровня агрессивности.

Для выявления всех возможных разновидностей высокоуровневых атак система должна иметь модульную структуру, при которой каждый модуль реализует защиту от одного определенного вида атак. В итоге формируется интегральная оценка и делается вывод о допустимости или недопустимости передачи исследуемой части трафика пользователю

Выводы.

Разработанная система защиты была реализована на одной рабочей станции под управлением ОС Ubuntu Linux 9.10. В ходе исследований было установлено, что защищаемый хост устойчив к большинству видов сканирования портов, таких как SYN, ACK и FIN, а также к сканированию соединением. При этом доступ к глобальной сети интернет не нарушался и хост продолжал корректно обрабатывать запросы, отвечающие требованиям протоколов TCP/IP

Полученный пакетный фильтр позволяет защитить рабочую станцию от сетевой атаки на раннем этапе сканирования портов.

Список литературы

1. Ford J. L. “Absolute beginners guide to personal firewalls”, Indiana, Que publishing, 2002 – 272p.
2. Фленов М.Е. “Linux глазами хакера” – Санкт Петербург «БХВ-Петербург», 2005г. – 544 с.
3. Стивенс У.Р. «Unix. Разработка сетевых приложений. Мастер-класс»- Москва, «Питер», 2003 – 1040с.