Образовательный комплекс

Компьютерные сети

Лекция 17

Сетевая безопасность

Microsoft®

Содержание

- Сетевая безопасность – проблемы, механизмы, сервисы
- Фильтрация пакетов

Сетевая безопасность
Проблема безопасности

- В отсутствии защиты компьютерная сеть подвержена сетевым атакам самого различного типа
  - Прослушивание (sniffing) – перехват передаваемой по сети информации
  - Наличие посредника (man-in-the-middle), способного просматривать содержимое трафика и изменять его
  - Подделка источника (spoofing) – передача данных от чужого имени
  - Компрометация пользователя – получение идентификационной информации пользователя, возможность доступа к ресурсам от его имени
  - Отказ в обслуживании (denial of service, DOS) – перегрузка или блокирование сервиса
  - …

Сетевая безопасность
Общие термины…

- Защита информации – комплекс мероприятий, проводимых с целью недопущения утраты, искажения, утечки, блокирования информации и т.д.
- Безопасность информации дополнительно включает аутентификацию, аудит, обнаружение проникновения и т.п.

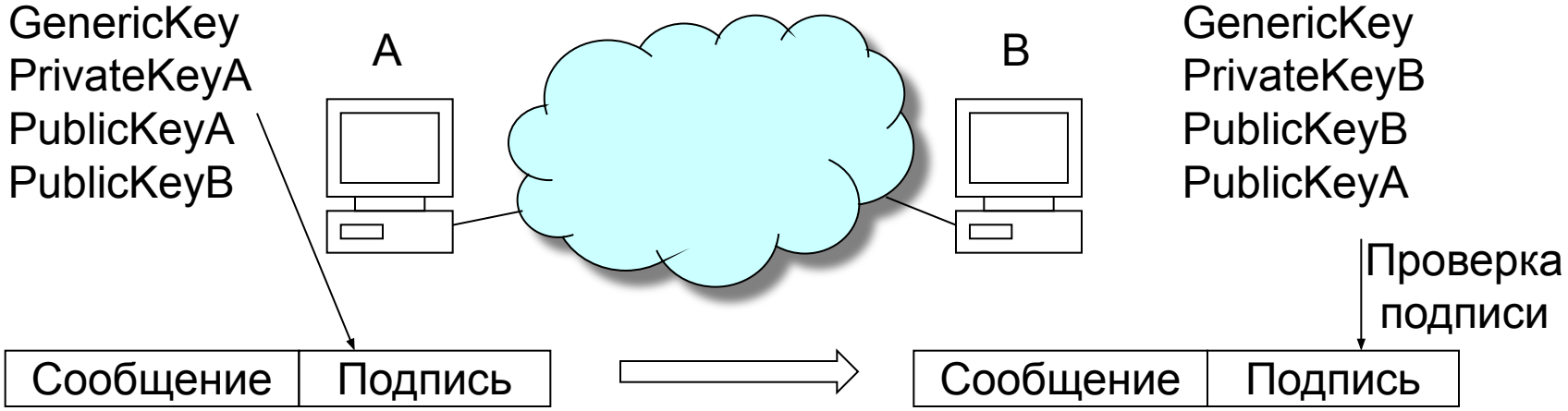
Сетевая безопасность
Общие термины

- Компрометация – действия, в результате выполнения которых объект компрометации становится небезопасным
  - Получения имени и пароля учетной записи пользователя сторонним лицом – компрометация учетной записи
  - Изменение передаваемых данных – компрометация данных
- Атака – действие, направленное на компрометацию какого-либо объекта
- Уязвимость – (слабое) место в системе (аппаратное или программное), которое может быть атаковано
- Механизм безопасности – аппаратное или программное средство, защищающее уязвимости от атак
- Политика безопасности – порядок защиты информации в организации (контролирует порядок хранения, обработки и обмена информацией)
- Сервис безопасности – комплекс аппаратных и программных средств, реализующих политику безопасности

Сетевая безопасность
Механизмы безопасности

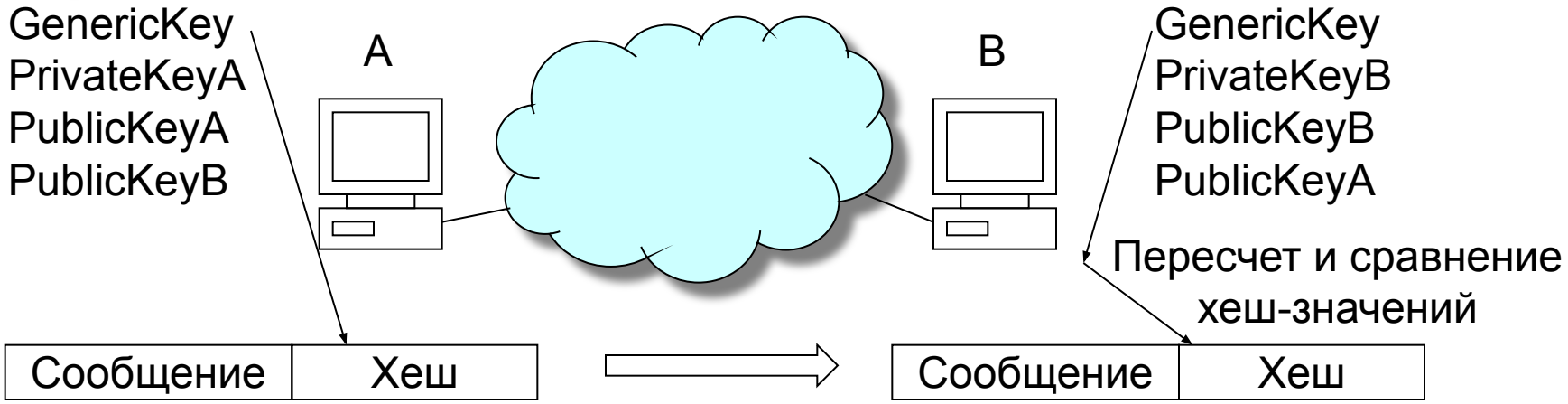
- Симметричные алгоритмы шифрования – используют один и тот же ключ для шифрования и дешифрования
- Асимметричные алгоритмы шифрования – используют различные ключи для шифрования и дешифрования
  - Как правило, используется пара "открытый" (публичный, public) ключ и "закрытый" (секретный, private) ключ, "открытый" ключ может получен из "закрытого", но не наоборот
  - Сервис может сформировать пару ключей и распространить открытый ключ для организации безопасного взаимодействия
- Хеш-функции вычисляют по сообщению произвольной длины значение фиксированного размера
  - Позволяют с большой вероятностью определять наличие изменений в передаваемом сообщении
  - Используют симметричные ключи (то есть отправитель и получатель должны знать ключ хеширования)

Сетевая безопасность
Сервисы безопасности…



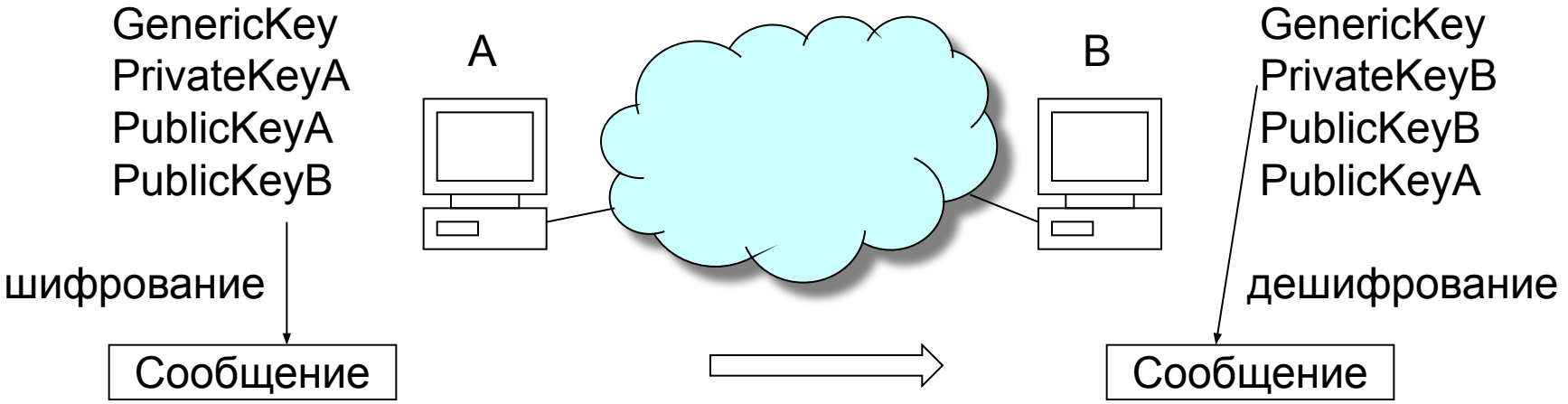
- Неотрекаемость (non-repudiation) – гарантирует подлинность отправителя сообщения
  - Отправитель может добавлять к сообщению цифровую подпись, сформированную с помощью своего секретного ключа
  - Получатель может проверить подлинность сообщения, используя открытый ключ отправителя

Сетевая безопасность
Сервисы безопасности…



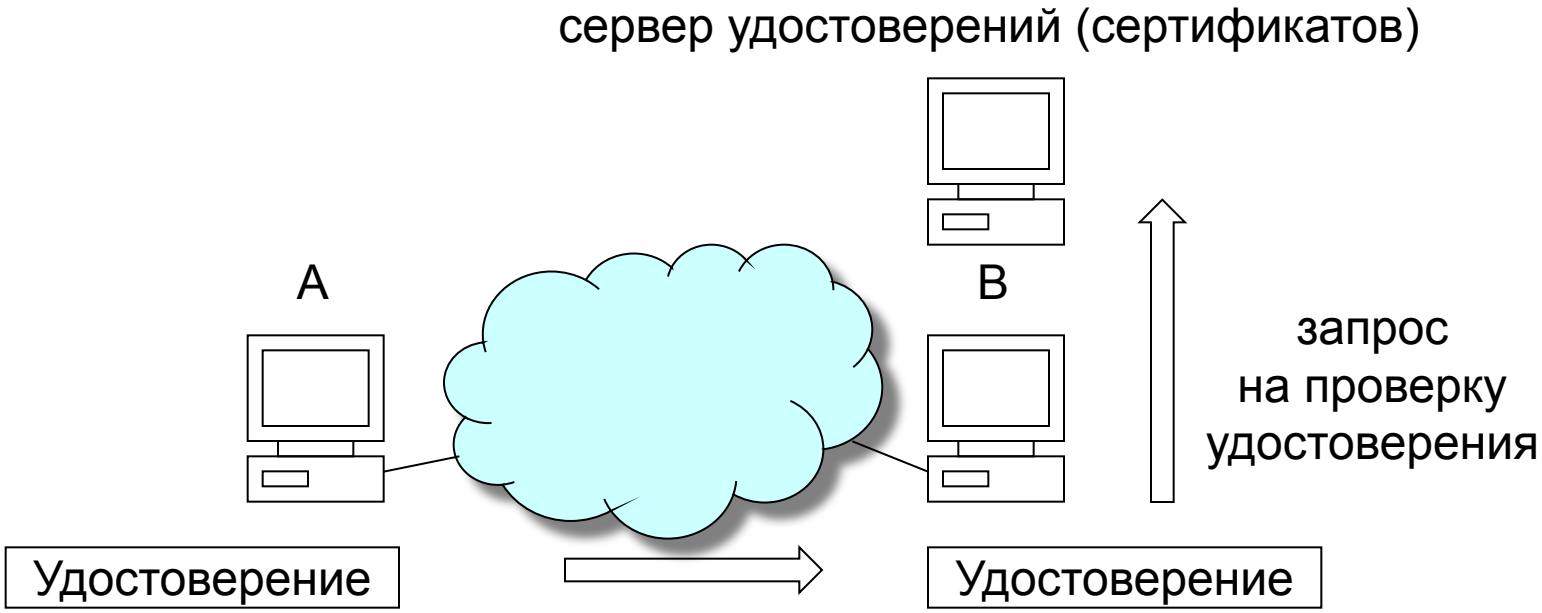
- Целостность (integrity) – гарантирует, что информация при передаче не была изменена
  - Для сообщений вычисляется значение хеш-функции, оно записывается в сообщение и проверяется получателем
  - Требуется, чтобы отправитель и получатель имели общий ключ

Сетевая безопасность
Сервисы безопасности…



- Конфиденциальность (confidentiality) – гарантирует возможность раскрытия данных только получателем
  - Источник шифрует данные открытым ключом получателя, получатель дешифрует данные, используя свой секретный ключ

Сетевая безопасность Сервисы безопасности…



- Аутентификация (authentication) – гарантия того, что взаимодействующие стороны действительно являются теми, за кого себя выдают
  - Подлинность может подтверждаться посредством посылки каждой стороной своего удостоверения (сертификата) и проверки его легитимности другой стороной

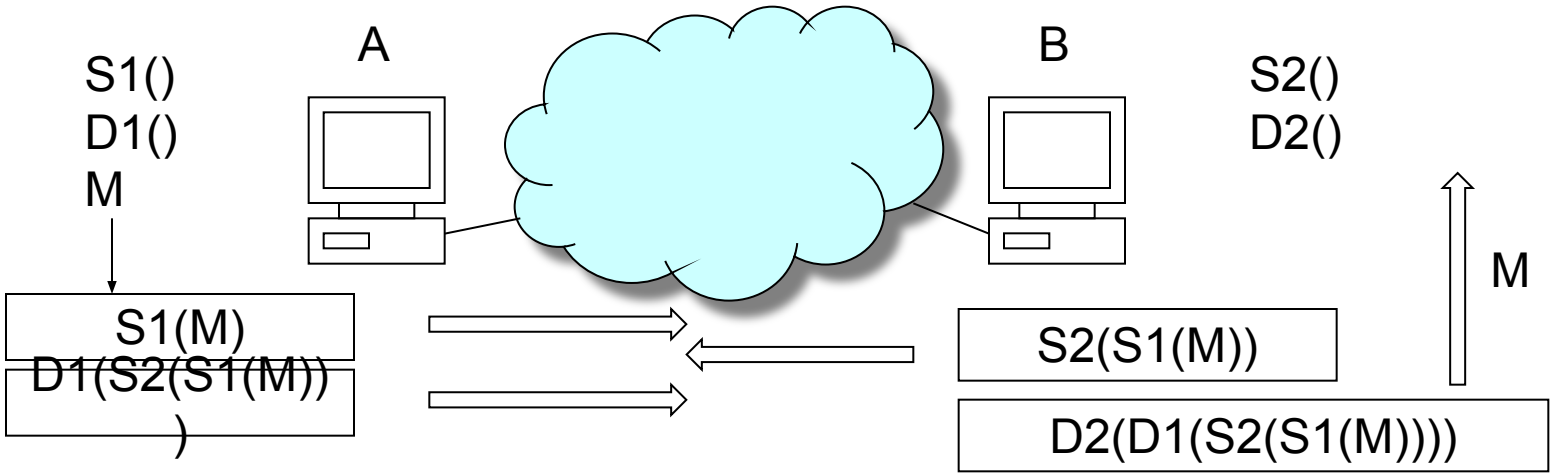
Сетевая безопасность
Сервисы безопасности

- Защита от повторений (replay prevention) – обеспечивает уникальность каждого сообщения
  - Например, можно для каждого IP-пакета указывать уникальный номер с момента последней смены ключей в установленном соединении
  - Требуется для того, чтобы узел, который мог получить передаваемый пакет, не смог воспользоваться им впоследствии для установления сеанса с получателем
- Контроль доступа – позволяет ограничить и контролировать доступ к ресурсам

Сетевая безопасность
Обмен ключами…

- Обмен открытыми ключами можно проводить без шифрования
  - Достаточно выполнить аутентификацию другой стороны
- Для передачи секретного ключа можно использовать алгоритмы шифрования, допускающие произвольный порядок дешифрования
  - Пусть M-шифруемое сообщение, S1() и S2() – функции шифрования, D1() и D2() – соответствующие им функции дешифрования
    - Как правило, это одни и те же пары функций, но использующие различные ключи
  - A = D1(S1(M)) = D2(S2(M)) = D2(D1(S1(S2(M)))) – естественные требования к функциям
  - A = D1(D2(S1(S2(M)))) – дополнительное требование
    - Пример: обмен ключами Диффи-Хеллмана

Сетевая безопасность
Обмен ключами



- Пример последовательности обмена
  - Узел А формирует секретный ключ М
  - А передает В сообщение, содержащее S1(M)
  - В передает А S2(S1(M))
  - А передает В D1(S2(S1(M)))
  - В вычисляет D2(D1(S2(S1(M)))) = A

Сетевая безопасность
Управление ключами

- Мы выяснили, что два субъекта могут безопасно обменяться ключами, но в реальности требуемое количество ключей в сети может быть очень велико
- В больших сетях часто используют центр распределения ключей (Key Distribution Center, KDC), отвечающий за распределение ключей между узлами и конкретными сервисами/приложениями
  - Каждый узел должен иметь свой общий ключ с KDC (мастер-ключ)
  - При установлении соединений приложения запрашивают для каждой сессии отдельный ключ (ключ сессии)

Сетевая безопасность IPSec

- IPSec (IP-Security) – IP-безопасность, основана на защите соединений "точка-точка" и реализует
  - защиту IP-пакетов
  - защиту от сетевых атак
- Использует протоколы
  - Encapsulated Security Payload (ESP) - защита данных IP-пакета путем шифрования содержимого с помощью симметричных криптографических алгоритмов (Blowfish, 3DES).
  - Authentication Header (AH) – защита заголовка IP-пакета путем вычисления криптографической контрольной суммы и хеширования полей заголовка IP пакета защищенной функцией хеширования
- Безопасное соединение (Security Association, SA) – базовое понятие IPSec, означающее однонаправленное (симплексное) логическое соединение, создаваемое для обеспечения безопасности
- Используется для непосредственного шифрования трафика между двумя хостами (транспортный режим) или для построения ''виртуальных туннелей'' между двумя подсетями (туннельный режим)
  - Последний случай обычно называют виртуальной частной сетью (Virtual Private Network, VPN)

Сетевая безопасность
Virtual Private Network…

- Описание ситуации
  - Имеется две сети
  - Внутри обеих сетей используется протокол IP
  - Сети имеют маршрутизаторы, соединенные друг с другом через Интернет
  - У маршрутизатора каждой из сетей есть как минимум один публичный IP-адрес
  - Внутренние IP-адреса сетей могут быть публичными или приватными (не имеет значения); на маршрутизаторах может работать сетевое преобразование адресов (Network Address Translation, NAT)
  - Внутренние IP-адреса двух сетей не должны пересекаться
- Необходимо организовать защищенную передачу данных между сетями через Интернет

Сетевая безопасность
Virtual Private Network

- Все пакеты, приходящие на VPN-сервер1 из сети 192.168.1.0/24 и направленные в сеть 192.168.2.0/24, инкапсулируются в пакеты ESP и отправляются через Интернет VPN-серверу2, который их извлекает и доставляет в сеть 192.168.2.0/24

Фильтрация пакетов

Фильтрация пакетов

- Фильтрация пакетов обычно делается на сетевом или транспортном уровне
  - каждый пакет проверяется на удовлетворение ряду условий
  - в зависимости от выполненных условий производится обработка пакета
- Фильтрация пакетов может выполняться на любом узле, но обязательно должна использоваться на маршрутизаторах, пограничных с Интернет
- Мы рассмотрим частный случай – фильтрация IP-пакетов посредством iptables (механизм фильтрации, реализованный в ядрах версий 2.4 и 2.6 ОС Linux)

Пакетный фильтр iptables
Признаки фильтрации

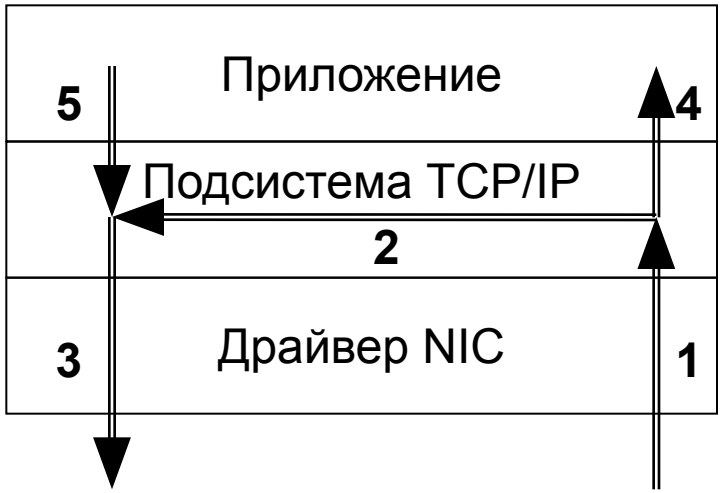
- iptables может анализировать
  - IP-адрес источника, IP-адрес получателя
  - Тип протокола
  - Номер порта источника, номер порта получателя (для протоколов TCP и UDP)
  - Флаги протокола TCP
  - Данные заголовка IP пакета
  - Признак того, что пакет является первым в последовательности
  - Другие параметры
- iptables не анализирует данные пакета

Пакетный фильтр iptables Фильтрация

- iptables при фильтрации использует последовательности (цепочки, chains) правил, каждое из которых содержит
  - набор условий
  - выполняемое действие
- Правила в цепочке просматриваются последовательно
  - Если условия применимы к обрабатываемому пакету, выполняется указанное в правилах действие
    - В зависимости от действия просмотр правил в цепочке завершается либо продолжается
  - Если условия не применимы к обрабатываемому пакету, переходим к следующему правилу в цепочке

Пакетный фильтр iptables
Цепочки

- Поддерживается 5 встроенных цепочек
  - 1 – PREROUTING
  - 2 – FORWARD
  - 3 – POSTROUTING
  - 4 – INPUT
  - 5 – OUTPUT
- Можно создавать пользовательские цепочки, но их использование явно определяется в правилах встроенных цепочек



Пакетный фильтр iptables Таблицы…

- Для различных типов обработки IP-пакетов существуют 3 таблицы (каждая из которых имеет индивидуальный набор цепочек)
  - filter – предназначена для задания правил фильтрации пакетов;
    - 4 – INPUT
    - 2 – FORWARD
    - 5 – OUTPUT
  - nat – предназначена для задания преобразования сетевых адресов (Network Address Translations, NAT); может использовать цепочки
    - 1 – PREROUTING
    - 3 – POSTROUTING
    - 5 – OUTPUT
  - mangle – предназначена для внесения изменений в заголовки пакетов; может использовать все цепочки

Пакетный фильтр iptables Таблицы

- При обработке пакетов порядок использования цепочек однозначно определен
  - Для транзитных пакетов
    - mangle – PREROUTING
    - nat – PREROUTING
    - mangle – FORWARD
    - filter – FORWARD
    - mangle – POSTROUTING
    - nat – POSTROUTING
  - Для пакетов, предназначенных локальному приложению
    - mangle – PREROUTING
    - nat – PREROUTING
    - mangle – INPUT
    - filter – INPUT
  - Для исходящих пакетов локальных приложений
    - mangle – OUTPUT
    - nat – OUTPUT
    - filter – OUTPUT
    - mangle – POSTROUTING
    - nat – POSTROUTING

Пакетный фильтр iptables
Утилиты

- Для управления правилами используется утилита iptables
  `iptables [opts] [-t table] [-com] [parms]`
  которая обеспечивает
  - Создание/удаление пользовательских цепочек
  - Задание политики по умолчанию для цепочки
  - Добавление/изменение/удаление правил
  - Просмотр/установку/сброс счетчиков пакетов
  - и т.д.
- По умолчанию используется таблица filter
- Утилиты iptables-save и iptables-restore позволяют сохранить конфигурацию в файл и восстановить ее из файла

Пакетный фильтр iptables Таблица filter…

- В таблице filter правила могут использовать условия отбора пакетов различных типов
  - Общие – не зависят от протокола
    - протокол
    - IP-адрес источника и IP-адрес получателя
    - входной и выходной NIC
  - Неявные – зависят от типа протокола
    - для TCP – номера портов источника и получателя и флаги TCP
    - для UDP – номера портов источника и получателя
    - для ICMP – тип сообщения ICMP
  - Явные – требуют загрузки специальных модулей
    - модуль mac позволяет проверять MAC-адреса узлов, передающих пакеты
    - модуль state отслеживает соединения между процессами и позволяет писать условия в терминах состояния соединения
    - модуль limit позволяет ограничить число срабатываний правила
    - и т.д.

Пакетный фильтр iptables Таблица filter

- В таблице filter правила могут использовать следующие действия
  - ACCEPT – пакет принимается для дальнейшей обработки
  - REJECT – пакет уничтожается, источнику посылается ICMP-сообщение
    - Можно явно в правиле указать тип отправляемого ICMP-сообщения
  - DROP – пакет уничтожается, ICMP-сообщение источнику не посылается
  - ИМЯ_ЦЕПОЧКИ – перейти к просмотру правил указанной цепочки
  - RETURN – вернуться к просмотру правил цепочки, из которой была запрошена обработка правил текущей цепочки
  - LOG – внести запись о срабатывании правила в журнал
  - существуют другие действия

Пакетный фильтр iptables
Таблица nat

- Преобразование сетевых адресов позволяет использовать во внутренней сети адреса из частного диапазона
  - При попытке отправить пакет из внутренней сети к внешнему узлу маршрутизатор подменяет IP-адрес источника своим внешним адресом
  - При приходе ответного пакета от внешнего узла IP-адрес получателя подменяется на внутренний IP-адрес узла, пославшего исходящий пакет, и пакет передается во внутреннюю сеть
- В таблице NAT правила могут использовать следующие действия
  - SNAT или MASQUERADE – замена IP-адреса и/или порта источника
  - DNAT – замена IP-адреса или порта назначения (используется для организации доступа из внешних сетей к серверам, расположенным во внутренней сети и имеющим адреса из частного диапазона)

Заключение

- В настоящий момент сетевая безопасность является одним из ключевых вопросов при планировании и реализации сетевой инфраструктуры; неудачное решение может существенно понизить надежность сетевой инфраструктуры
- При построении безопасных сетей используется множество аппаратно-программных решений, среди наиболее часто используемых – виртуальные частные сети и пакетные фильтры

Вопросы для обсуждения

Литература

- Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. М:ИНТУИТ.ру, 2005 г.
- Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server. – М.: Русская редакция, 2001.