Аппаратное и программное обеспечение ЭВМ и сетей

Тема_35_Сетевая безопасность. Основные понятия. Типы и примеры атак

Сетевая безопасность

- Наибольшую угрозу и опасность на сегодняшний день представляет глобальная сеть Интернет.
- Большая группа угроз связана с несовершенством протоколов TCP/IP. Эти протоколы разрабатывались в то время, когда проблема обеспечения информационной безопасности еще не стояла на повестке дня. Сообщество пользователей Интернета представляло собой ограниченный круг заинтересованных в эффективной работе Сети специалистов, и уж, конечно, никто не покушался на ее работоспособность. Создаваемые протоколы не содержали механизмов, позволяющих противостоять возможным атакам злоумышленников. Например, хотя в протоколах FTP и telnet и предусмотрена аутентификация, клиент передает пароль серверу по сети в незашифрованном виде, а значит, злоумышленник может перехватить его и получить доступ к FTP-архиву.
- Многообразие угроз порождает многообразие методов защиты. В этой лекции мы будем обсуждать основные понятия сетевой безопасности и типы и примеры атак.

Основные понятия информационной безопасности

Определение безопасной системы

- Под ***информационной безопасностью*** понимается состояние защищенности информационной системы, включая собственно информацию и поддерживающую ее инфраструктуру.
- Информационная система находится в **состоянии защищенности**, если обеспечены ее ***конфиденциальность, доступность и целостность***.
- **Конфиденциальность** (confidentiality) — это гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен; такие пользователи называются легальными, или авторизованными.
- **Доступность** (availability) — это гарантия того, что авторизованные пользователи всегда получат доступ к данным.
- **Целостность** (integrity) — это гарантия сохранности данными правильных значений, которая обеспечивается запретом неавторизованным пользователям каким-либо образом изменять, модифицировать, разрушать или создавать данные.
- Требования безопасности могут меняться в зависимости от назначения информационной системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой были бы не важны свойства целостности и доступности, но свойство конфиденциальности не всегда является обязательным.

Основные понятия информационной безопасности

- Например, если информация в Интернете на веб-сервере для общего доступа, то конфиденциальность не требуется. Однако требования целостности и доступности остаются актуальными.
- Понятия конфиденциальности, доступности и целостности определяются и к другим ресурсам вычислительной сети, таким как внешние устройства (принтер, модем, оборудование wi-fi (настройки)) или приложения.
- Свойство доступности устройства означает его готовность к работе, а свойство целостности может быть определено как свойство неизменности параметров данного устройства.
- Важна также легальность использования сетевых устройств. Устройства могут предоставлять различные услуги (распечатка текстов, отправка факсов, доступ в Интернет, электронная почта и т. п.). Незаконное использование, которых, наносит материальный ущерб предприятию, что также является нарушением безопасности системы.

Основные понятия информационной безопасности

Угроза, атака, риск

- **Угроза** — любое действие, которое может быть направлено на нарушение информационной безопасности системы.
- **Атака** — реализованная угроза.
- **Риск** — вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.
- Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников. Согласно статистики примерно 2/3 от общего числа всех инцидентов, составляют нарушения со стороны легальных пользователей сетей.
- *Угрозы со стороны легальных пользователей* делятся на:
  - умышленные;
  - неумышленные.

К умышленным угрозам относятся:

- Мониторинг - «подслушивание» внутри сетевого трафика с целью получения идентификаторов, паролей или конфигурационных параметров оборудования;

Умышленные и неумышленные угрозы.

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- злонамеренное получение доступа к конфиденциальным данным с целью их похищения, искажения или уничтожения;
- прямое «вредительство» — вывод из строя сетевого программного обеспечения и оборудования физически или с помощью программ вирусов;

нарушение персоналом правил пользователей в сети:

✔ посещение запрещенных веб-сайтов,

✔ вынос за пределы предприятия съемных носителей,

✔ небрежное хранение паролей и др.

- *Неумышленные угрозы - это* нарушения персонала:
- ошибки, лояльных сотрудников (низкая квалификации или безответственность) приводящих к повреждению сетевых

Угрозы внешних злоумышленников

- *Угрозы внешних злоумышленников*, называемых также хакерами, по определению являются умышленными и квалифицируются как преступления. Целью, внешних угроз нанесение вреда предприятию или конкретному лицу. Это может быть, например, получение конфиденциальных данных, которые могут быть использованы для снятия денег с банковских счетов, или установление контроля над программно-аппаратными средствами сети для последующего их использования в атаках на сети других предприятий.
- Для проведения атаки хакеры, как правило, занимаются *сбором информации о системе* (mapping). Это типы операционных систем и сетевых приложений, IP-адреса, номера портов клиентских частей приложений, имена и пароли пользователей. Часть информации такого рода может быть получена путем простого общения с персоналом (это называют социальным инжинирингом), а часть — с помощью тех или иных программ. Для подготовки и проведения атак используются либо специально разработанные программные средства, либо легальные программы мониторинга и диагностики сети, такие как: ping, tracert, nslookup, net xxxx и другие.

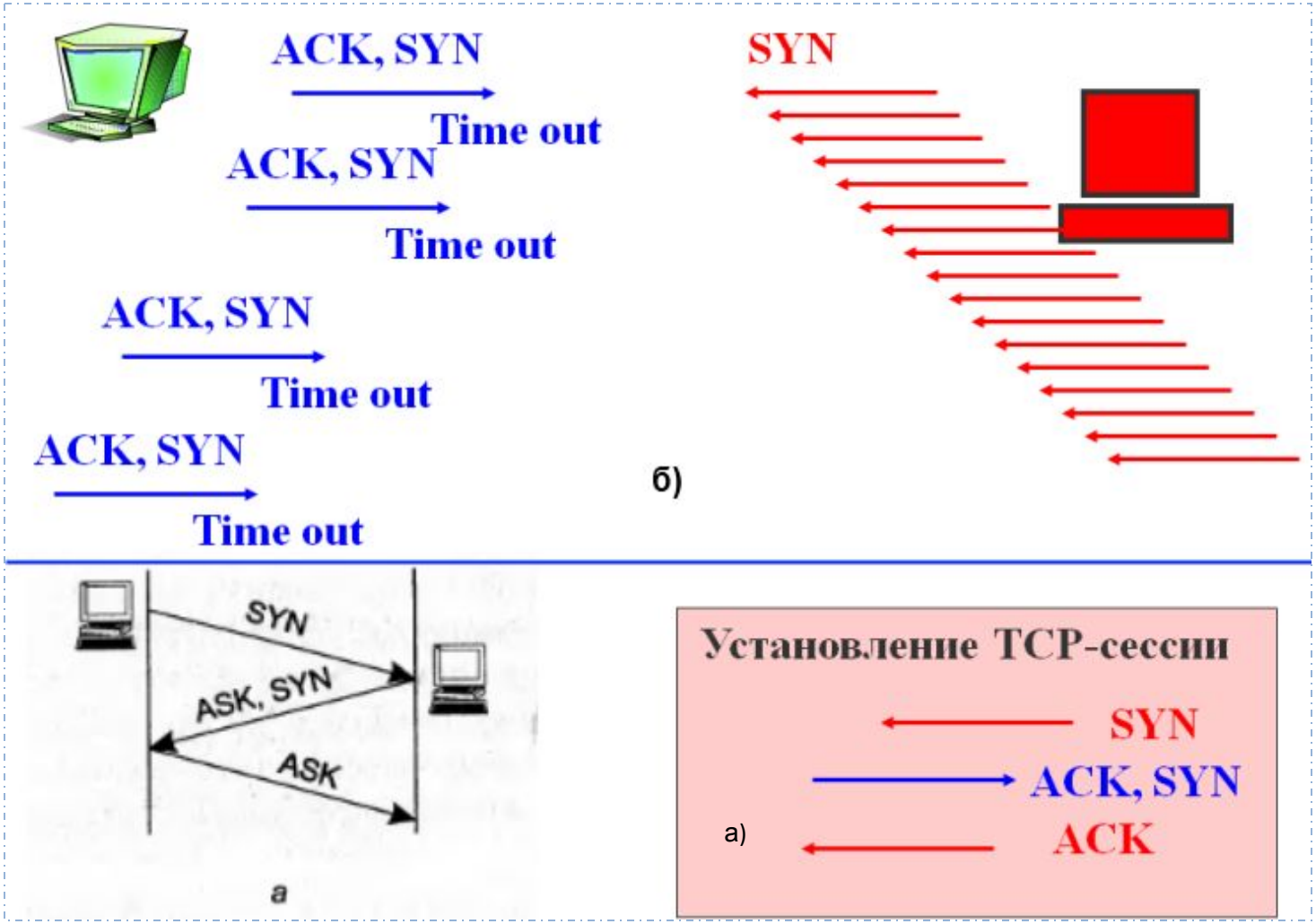
Основные понятия информационной безопасности

- При проведении атаки, злоумышленники часто прибегают к *подмене содержимого пакетов* (spoofing), в частности, изменяют значение поля адреса отправителя в заголовках пакетов.
- Для установления контроля, завладения информацией или просто для нанесения вреда, хакеры часто применяют такой вид атаки как, отказ в обслуживании (Denial of Service, DoS). Чаще всего объектами DOS-атак становятся основные веб-серверы, файловые и почтовые серверы предприятия, а также корневые серверы системы DNS.
- Для проведения DoS-атак злоумышленники часто координируют «работу» нескольких компьютеров. В таких случаях имеет место распределенная атака отказа в обслуживании (Distributed Denial of Service, DDoS).
- Злоумышленник, захватив управление над группой удаленных компьютеров, «заставляет» их посылать пакеты в адрес узла-жертвы (рис. 6-35.1). Получившийся в результате мощный суммарный поток «затопляет» атакуемый компьютер, вызывая его перегрузку и, в конечном счете, делает его недоступным. Блокировка происходит в результате исчерпания ресурсов либо процессора, либо операционной системы, либо канала связи (полосы пропускания).

Типы и примеры атак DOS атака.

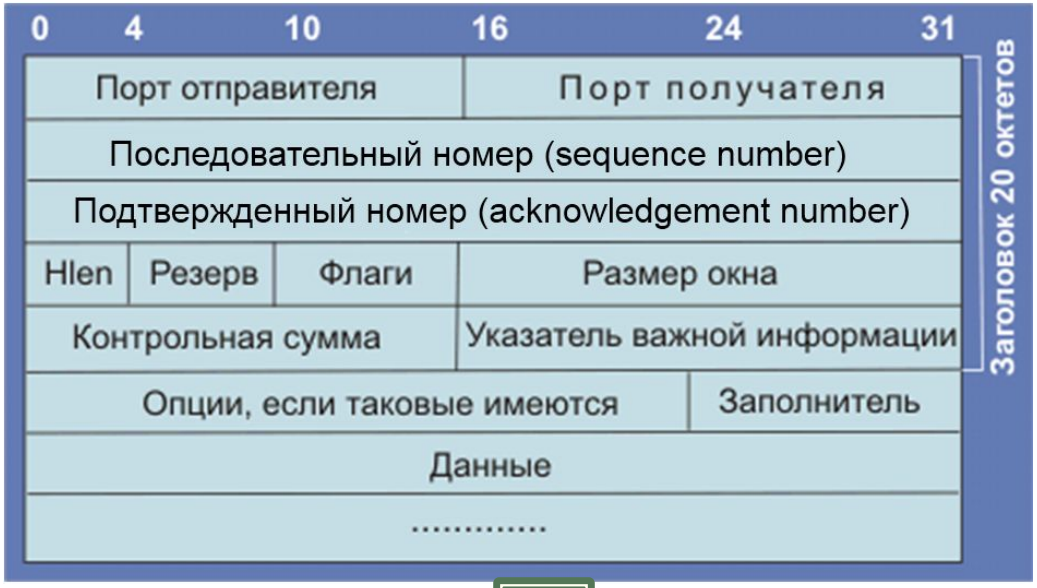
- Для выполнения DOS атаки злоумышленник организует передачу на сервер массированного потока пакетов с флагом *SYN,* каждый из которых инициирует создание нового TCP-соединения (рис. 6-35.2, *б).* Получив пакет с флагом *SYN,* сервер выделяет для нового соединения необходимые ресурсы и в полном соответствии с протоколом отвечает клиенту пакетом с флагами *ACK* и *SYN.* После этого, установив тайм-аут, он начинает ждать от клиента завершающий пакет с флагом *ACK,* который, увы, так и не приходит. Аналогичным образом создается множество других «недоустановленных» соединений. В результате возникает перегрузка сервера, все его ресурсы идут на поддержание множества соединений, процедуры установления которых остались незавершенными. В таком состоянии сервер уже не способен отвечать на запросы..
- Вызвать перегрузку ресурса сети можно также используя уязвимости и ошибки ОС, т.е. атака может быть осуществлена путем передачи потока запросов, синтаксически правильных, но специально сконструированных, так, чтобы вызвать перегрузку
- Например: так, для некоторых версий веб-сервера Apache губительным оказывается поток запросов, каждый из которых содержит большое количество заголовков HTTP или символов **«/»**.

Типы и примеры атак



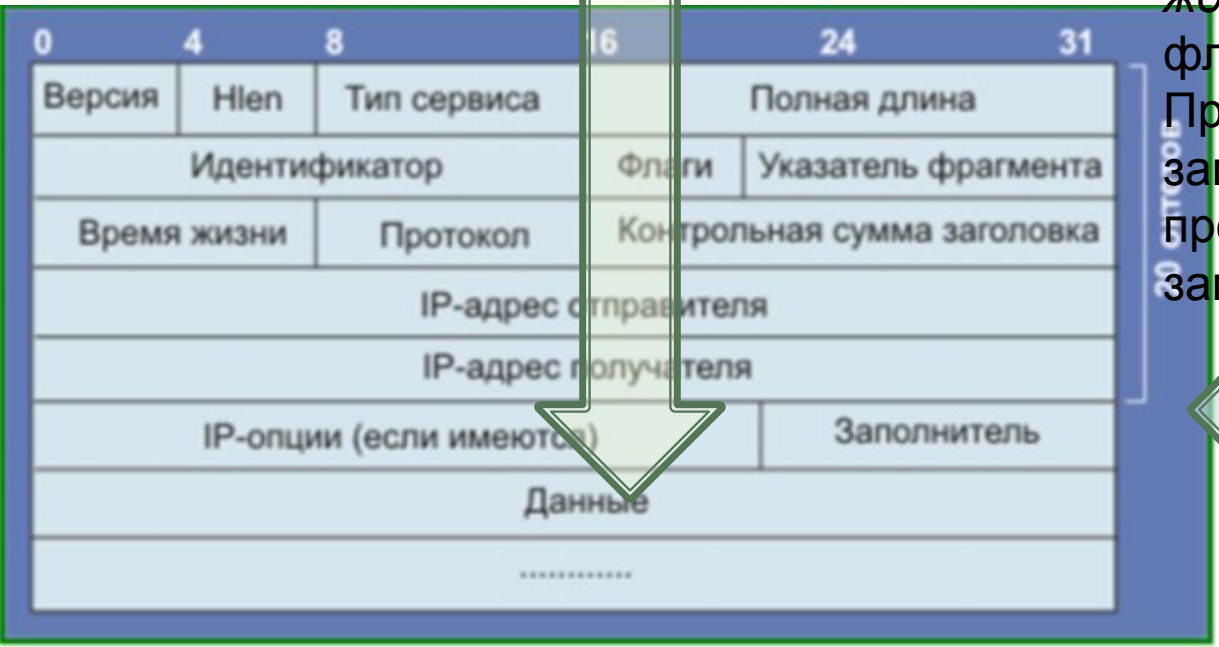
- **Рис. 6-35.2.** Проведение DoS-атаки, в которой используются особенности протокола TCP а) — нормальный порядок установления TCP- соединения; б) — DDoS-атака за счет создания множества незакрытых TCP-соединений.

Протокол транспортного уровня TCP



Пакет TCP протокола

Хакер использует свойства TCP протокола при установлении соединения, путем передачи массированного потока пакетов с флагом SYN, сервер отвечает пакетом с флагами *ACK* и *SYN и ждет от клиентов* пакеты с флагом ACK, но клиент молчит. При огромном количестве запросов сервер стопорится и прекращает отвечать на запросы.



Пакет IP протокола

Поля заголовка TCP-сегмента (продолжение)

Флаги Управляющие биты (**code bits**) числом 6 содержат служебную информацию о типе данного сегмента. Положительное значение сигнализируется установкой этих битов в единицу:

1) **URG** — срочное сообщение;
2) **ACK** — квитанция на принятый сегмент;
3) **PSH** — запрос на отправку сообщения без ожидания заполнения буфера (протокол TCP может выжидать заполнения буфера перед отправкой сегмента, но если требуется срочная передача, то приложение сообщает об этом протоколу TCP с помощью данного бита);
4) **RST** — запрос на восстановление соединения;
5) **SYN** — сообщение, используемое для синхронизации счетчиков переданных данных при установлении соединения;
6) **FIN** — признак достижения передающей стороной последнего байта в потоке передаваемых данных.

Типы и примеры атак

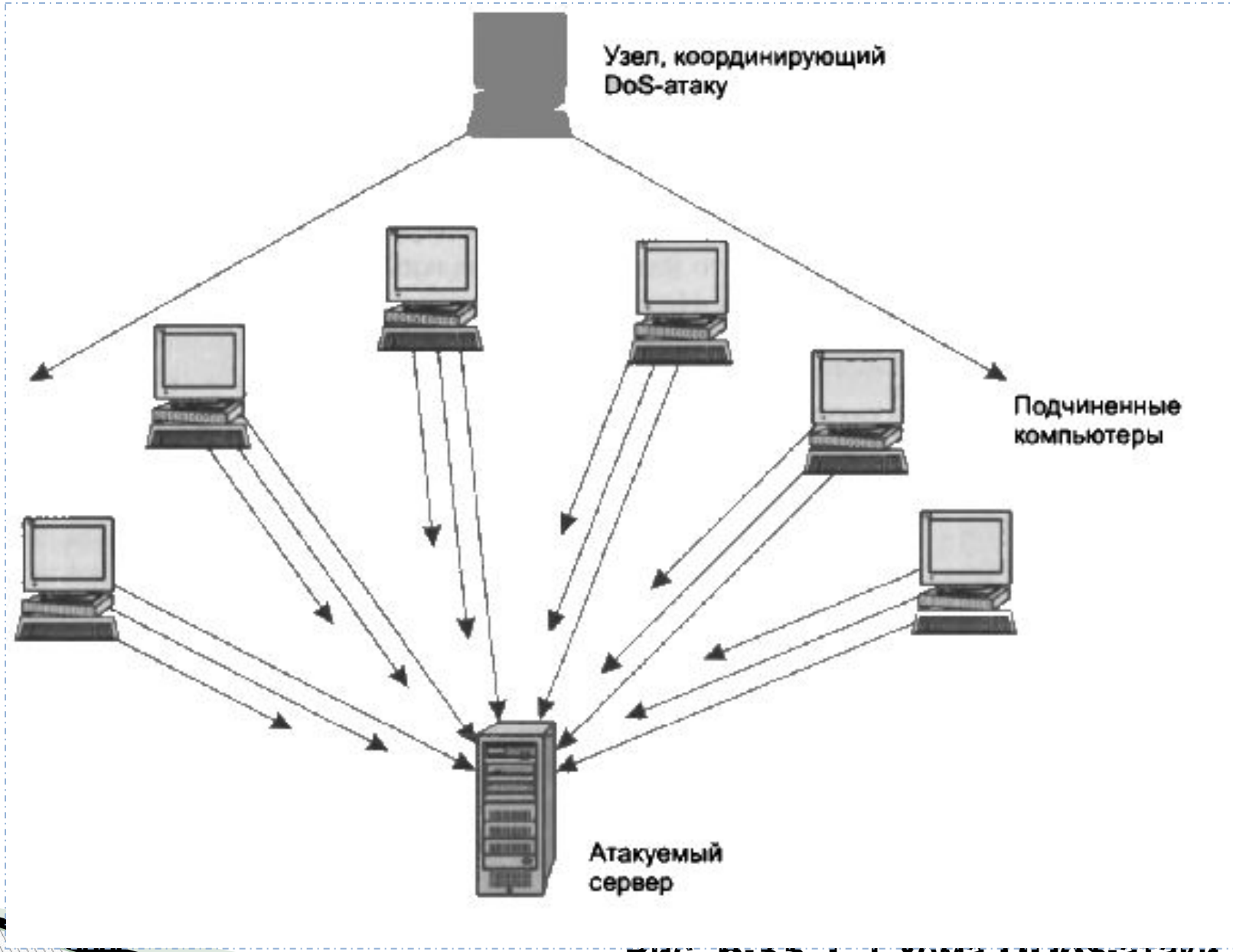
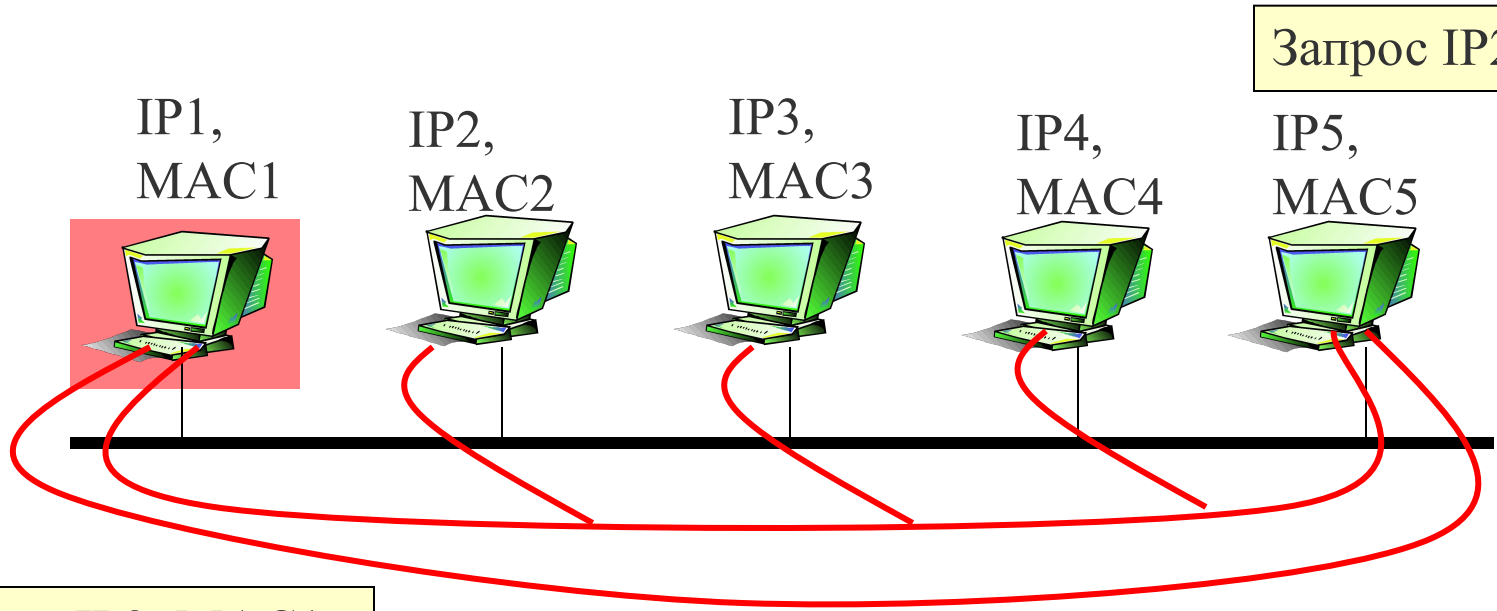


Рис. 6-35.1. Схема DDoS-атаки

Ложный ARP-ответ



Типы и примеры атак

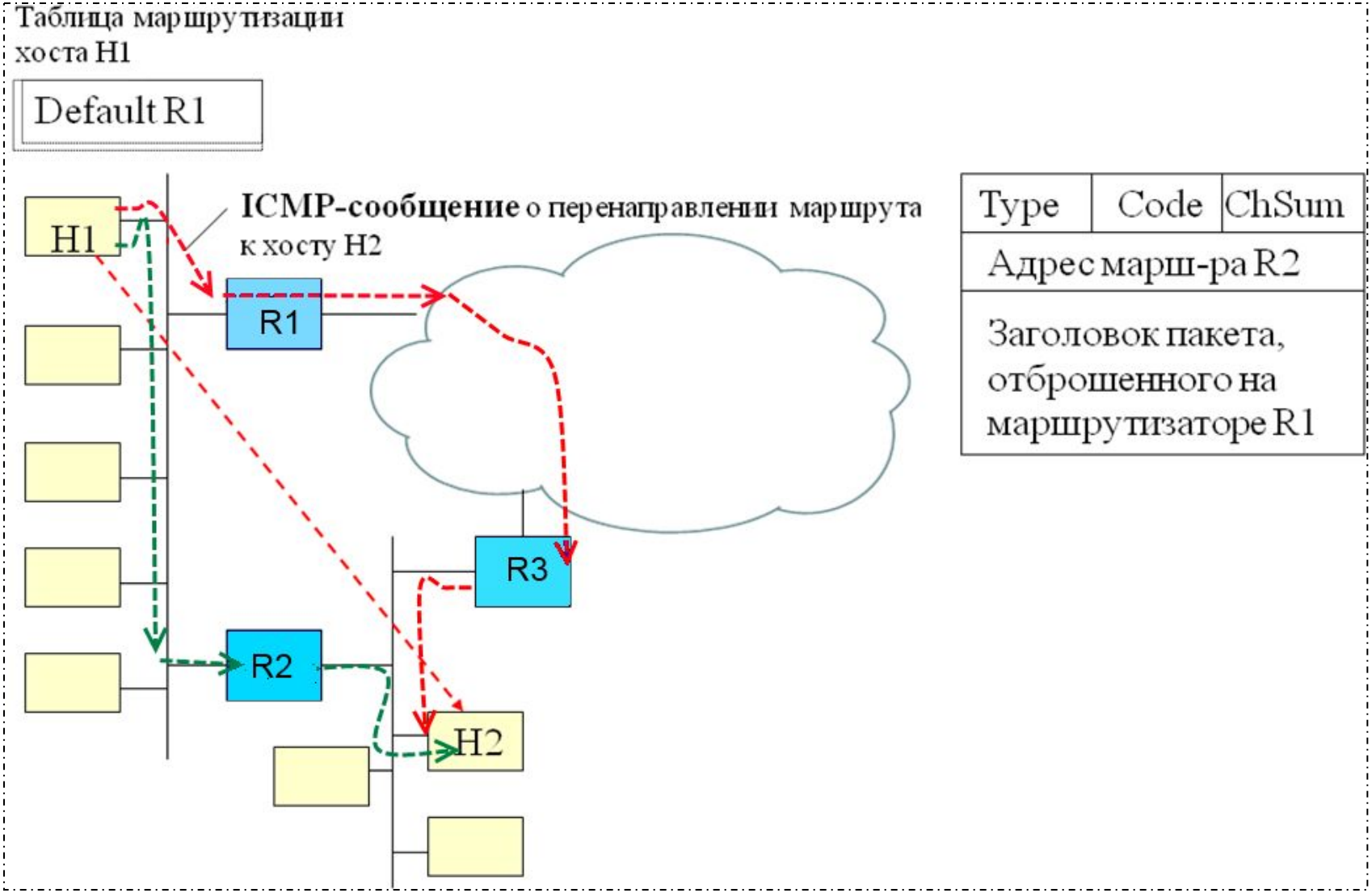
Перехват и перенаправление трафика

- Следующий тип атак – перехват трафика атакуемого компьютера или перенаправление по ложному адресу, в качестве которого может выступать адрес либо злоумышленника, либо третьей стороны. Пользовательским потоком данных злоумышленник может распорядиться двумя способами:
- ***Первый*** состоит в том, что злоумышленник маскируется под сервера адресата, передавая клиенту ту «картинку» и те сообщения, которые тот ожидает. Таким образом, злоумышленник может завладеть идентификатор и пароль пользователя. Эти данные в дальнейшем могут применяться для несанкционированного доступа к серверу предприятия или банка, которые и являются главной целью атаки.
- ***Второй*** способ заключается в организации транзита трафика. Каждый перехваченный пакет запоминается и/или анализируется на атакующем узле, а после этого перенаправляется на «настоящий» сервер.
- В обоих случаях, весь трафик между клиентом и сервером пропускается через компьютер злоумышленника и контролируется им.
- Рассмотрим некоторые приемы проведении атак данного типа. Для большинства из них уже разработаны средства противодействия, и приводимые здесь описания атак носят в основном учебный характер.

Перехват и перенаправление трафика

- Если злоумышленник находится в пределах локальной или корпоративной сети, то один из вариантов перенаправления трафика может быть осуществлен путем отправки в сеть *ложного ARP-ответа.* В данном случае схема очевидна: получив широковещательный ARP-запрос относительно некоторого IP-адреса, злоумышленник посылает ложный ARP-ответ, в котором сообщается, что данному IP-адресу соответствует его собственный MAC-адрес. Рис 6-35.3
- Второй вариант перехвата и перенаправления трафика в – это использование сообщение протокола ICMP *о перенаправлении маршрута*. В соответствии с данным протоколом *ICMP-сообщение о перенаправлении маршрута.* Такое сообщение может послать маршрутизатор хосту непосредственно присоединенной локальной сети при отказе этого маршрута или, когда обнаруживает, что для некоторого адреса назначения хост использует нерациональный маршрут.
- На рис. 6-35.4, *а* применяемый по умолчанию маршрутизатор R1, получив от хоста H1 пакет, адресованный хосту H2, определяет, что наилучший маршрут к хосту H2 пролегает через другой маршрутизатор данной локальной сети, а именно через маршрутизатор R2. Маршрутизатор R1 отбрасывает полученный пакет и помещает его заголовок в ICMP-сообщение о перенаправлении маршрута, которое посылает хосту H1. (см.Примеч)

Типы и примеры атак

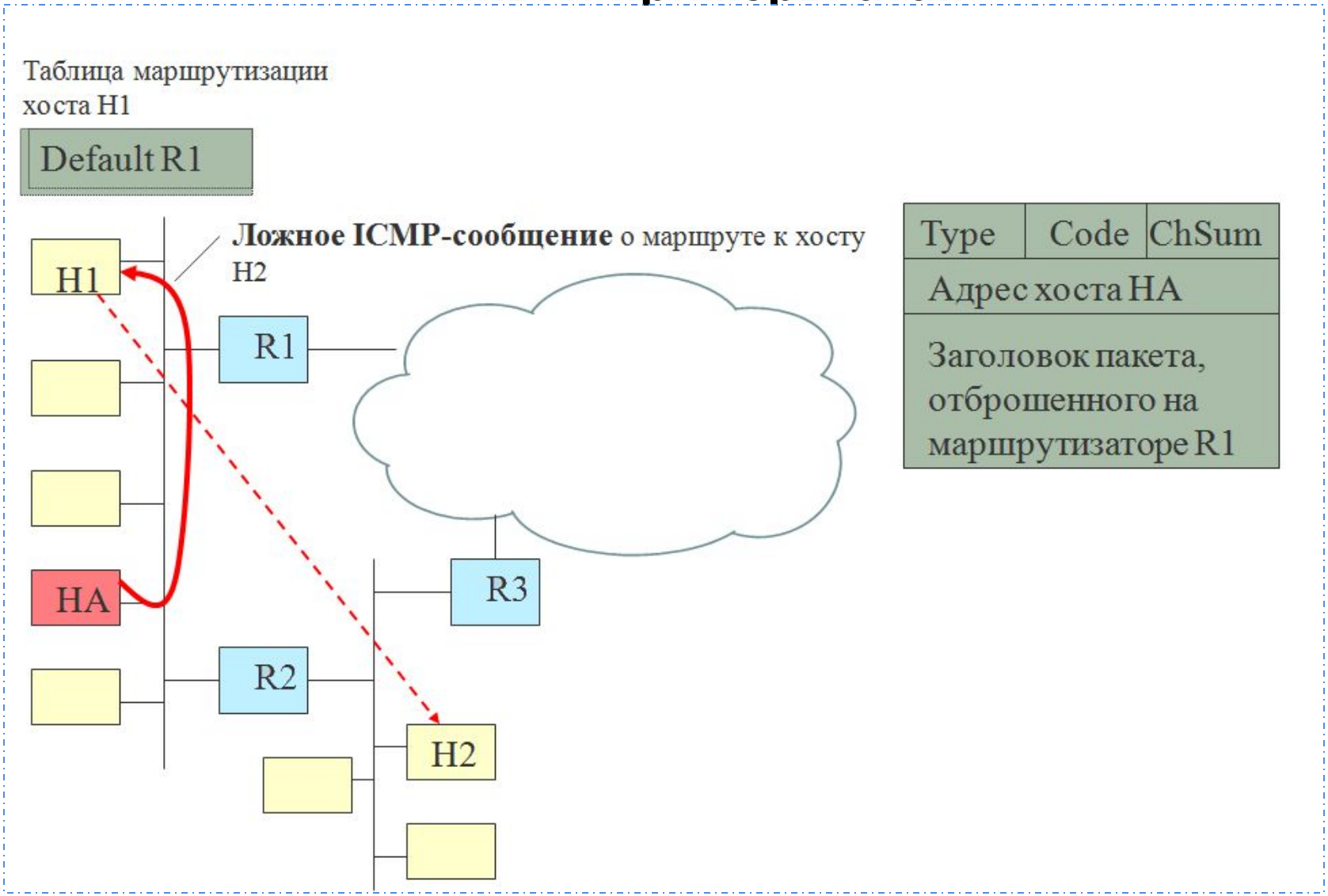


- **Рис. 6-35.4. а)** Перенаправление маршрута с помощью протокола ICMP: а — сообщение о более рациональном маршруте хосту H2 посылает маршрутизатор R1, применяемый по умолчанию;

Типы и примеры атак

- Для перехвата трафика, направляемого хостом H1 хосту H2, злоумышленник должен сформировать и послать хосту H1 пакет, маскирующийся под ICMP-сообщение о перенаправлении маршрута (рис. 6-35.3, б). В этом сообщении содержится запрос о корректировке таблицы маршрутизации хоста H1, так чтобы во всех пакетах с адресом IP_{H2} адресом следующего маршрутизатора стал адрес $IP_{\mathbf{HA}}$, являющийся адресом хоста-злоумышленника HA. Для того чтобы хост «поверил» этому сообщению, в поле IP-адреса отправителя должен быть помещен адрес маршрутизатора R1, являющегося маршрутизатором по умолчанию. Когда пакеты, передаваемые введенным в заблуждение хостом, начнут поступать на узел злоумышленника, он может либо захватывать и не передавать эти пакеты дальше, имитируя для поддержания диалога приложение, которому эти пакеты предназначались, либо организовать транзитную передачу данных по указанному адресу назначения IP_{H2}
- Читая весь трафик между узлами H1 и H2, злоумышленник получает все необходимую информацию для несанкционированного доступа к серверу H2.

Типы и примеры атак



- **Рис. 6-35.3. б)** Навязывание ложного маршрута б — сообщение о перенаправлении маршрута на себя направляет атакующий хост HA

Типы и примеры атак

- Еще одним способом перехвата трафика является использование *ложных DNS-ответов* (рис. 6-35.4). Задача злоумышленника состоит в получении доступа к корпоративному серверу. Для этого ему нужно завладеть именем и паролем авторизованного пользователя корпоративной сети. Эту информацию он решает получить путем ответвления потока данных, которые корпоративный клиент посылает корпоративному серверу. Злоумышленник знает, что клиент обращается к серверу, указывая его символьное DNS-имя www.example.com. Известно ему также, что перед тем как отослать пакет серверу, программное обеспечение клиентской машины направляет запрос DNS-серверу, чтобы узнать, какой IP-адрес соответствует этому имени.
- Цель злоумышленника — опередить ответ DNS-сервера и навязать клиенту свой вариант ответа, в котором вместо IP-адреса корпоративного сервера (в примере 193.25.34.125) злоумышленник указывает IP-адрес атакующего хоста (203.13.1.123). На пути реализации этого плана имеется несколько серьезных препятствий.

Типы и примеры атак

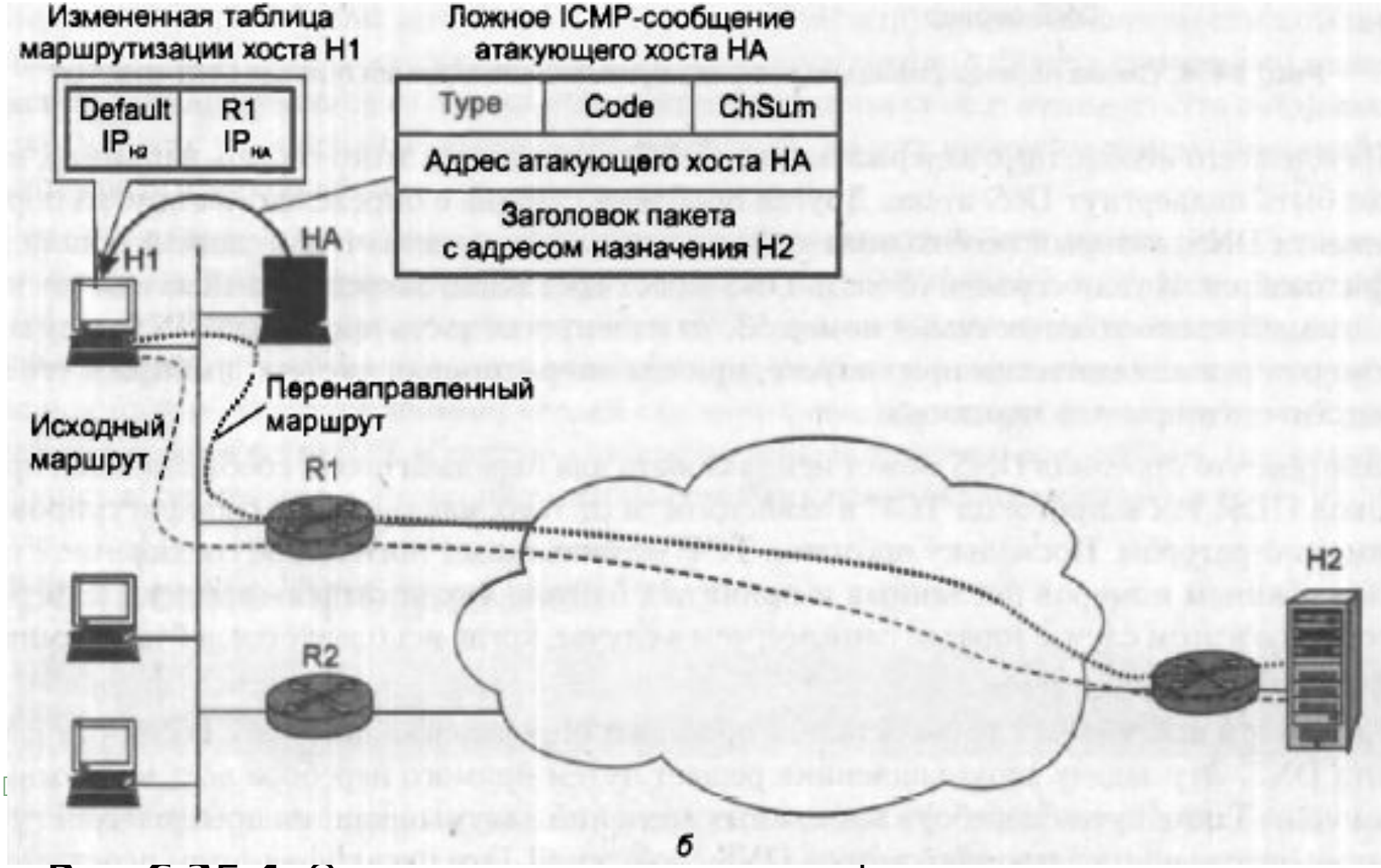


Рис. 6-35.4. Схема перенаправления трафика путем использования ложных DNS-ответов.

Типы и примеры атак

- Прежде всего, необходимо задержать ответ DNS-сервера, для этого сервер, например, может быть подвергнут DoS-атаке. Другая проблема связана с определением номера порта клиента DNS, который необходимо указать в заголовке пакета, чтобы данные дошли до приложения. И если серверная часть DNS имеет постоянно закрепленный за ней так называемый «хорошо известный» номер 53, то клиентская часть протокола DNS получает номер порта динамически при запуске, причем операционная система выбирает его из достаточно широкого диапазона. Заметим, что протокол DNS может использовать для передачи своих сообщений как протокол UDP, так и протокол TCP, в зависимости от того, как он будет сконфигурирован администратором. Поскольку протокол TCP устанавливает логическое соединение с отслеживанием номеров посланных и принятых байтов, «вклиниться» в диалог клиента и сервера в этом случае гораздо сложнее, чем в случае, когда используется дейтаграммный протокол UDP.

Типы и примеры атак

Типы и примеры атак

- Однако и в последнем случае остается проблема определения номера UDP-порта клиента DNS. Эту задачу злоумышленник решает путем прямого перебора всех возможных номеров. Также путем перебора возможных значений злоумышленник преодолевает проблему определения идентификаторов DNS-сообщений. Эти идентификаторы передаются в DNS-сообщениях и служат для того, чтобы клиент системы DNS мог установить соответствие поступающих ответов посланным запросам. Итак, злоумышленник бомбардирует клиентскую машину ложными DNS-ответами, перебирая все возможные значения идентифицирующих полей так, чтобы клиент, в конце концов, принял один из них за истинный DNS-ответ. Как только это происходит, цель злоумышленника можно считать достигнутой — пакеты от клиента направляются на адрес атакующего хоста, злоумышленник получает в свое распоряжение имя и пароль легального пользователя, а с ними и доступ к корпоративному серверу.

Внедрение в компьютеры вредоносных программ

- Многочисленная группа атак связана с внедрением в компьютеры **вредоносных программ** (malware), к числу которых относятся ***троянские и шпионские программы, черви, вирусы, спам, логические бомбы и некоторые другие типы программ, нацеленные на нарушение информационной безопасности.***
- Эти программы могут проникать на атакуемые компьютеры разными путями. Самый простой из них — «самодоставка», когда пользователь загружает файлы из непроверенных источников (съемных носителей или веб-сайтов) либо беспечно открывает подозрительный файл, пришедший к нему по электронной почте. Не мало вредоносных программ, которые самостоятельно «размножаются», по сети без участия пользователей.
- Вредоносные программы могут не только уничтожить, исказить, похитить информацию, но также привести в нерабочее состояние программное обеспечение, а значит, и компьютер в целом, что приводит к значительным затратам времени и сил администраторов на обнаружение и распознавание атак, востановление, тестирование и перезагрузку систем.

Троянские программы

- **Троянские программы,** или **трояны** (trojan), — это разновидность вредоносных программ, которые наносят ущерб системе, *маскируясь* под какие-либо полезные приложения.
- Троянские программы могут применять в качестве прикрытия *знакомые* пользователю приложения, с которыми он работал и раньше, до появления в компьютере «троянского коня», либо принимает вид *нового* приложения, которое пытается заинтересовать пользователя-жертву какими-то своими якобы полезными функциями.
- Однако суть троянской программы и в том и в другом случаях остается вредительской: она может уничтожать или искажать информацию на диске, передавать данные (например, пароли) с «зараженного» компьютера на удаленный компьютер хакера, приводить в неработоспособное состояние, установленное на атакованном компьютере программное обеспечение, участвовать в проведении DoS-атак на другие удаленные компьютеры.
- Так, одна из известных троянских программ AIDS TROJAN DISK7, при запуске перемешивала символы в именах всех файлов и заполняла все свободное пространство жесткого диска. После этого программа от имени злоумышленника предлагала помощь в восстановлении диска, требуя взамен вознаграждение для автора этой программы.

Сетевые черви.

- **Сетевые черви** (worm) — это программы, способные к *самостоятельному распространению* своих копий среди узлов в пределах локальной сети, а также по глобальным связям, перемещаясь от одного компьютера к другому без пользователей сети.
- Большинство сетевых червей передаются в виде файлов и основным механизмом их распространения являются сетевые файловые службы. Так, червь может рассылать свои копии в виде вложений в сообщения электронной почты или путем размещения ссылок на зараженный файл на каком-либо веб-сайте.
- Однако существуют и другие разновидности червей, которые для своей экспансии используют более сложные приемы, например, связанные с ошибками («дырами») в программном обеспечении.
- ***Типичная программа-червь*** не удаляет и не искажает пользовательские и системные файлы, не портит содержимое баз данных, сообщений E-Mail, ***а наносит вред атакованным компьютерам путем потребления их ресурсов***.
- Главная цель и результат деятельности червя состоит в том, чтобы передать свою копию на максимально возможное число компьютеров. При этом для поиска компьютеров — новых потенциальных жертв — черви задействуют встроенные в них средства.

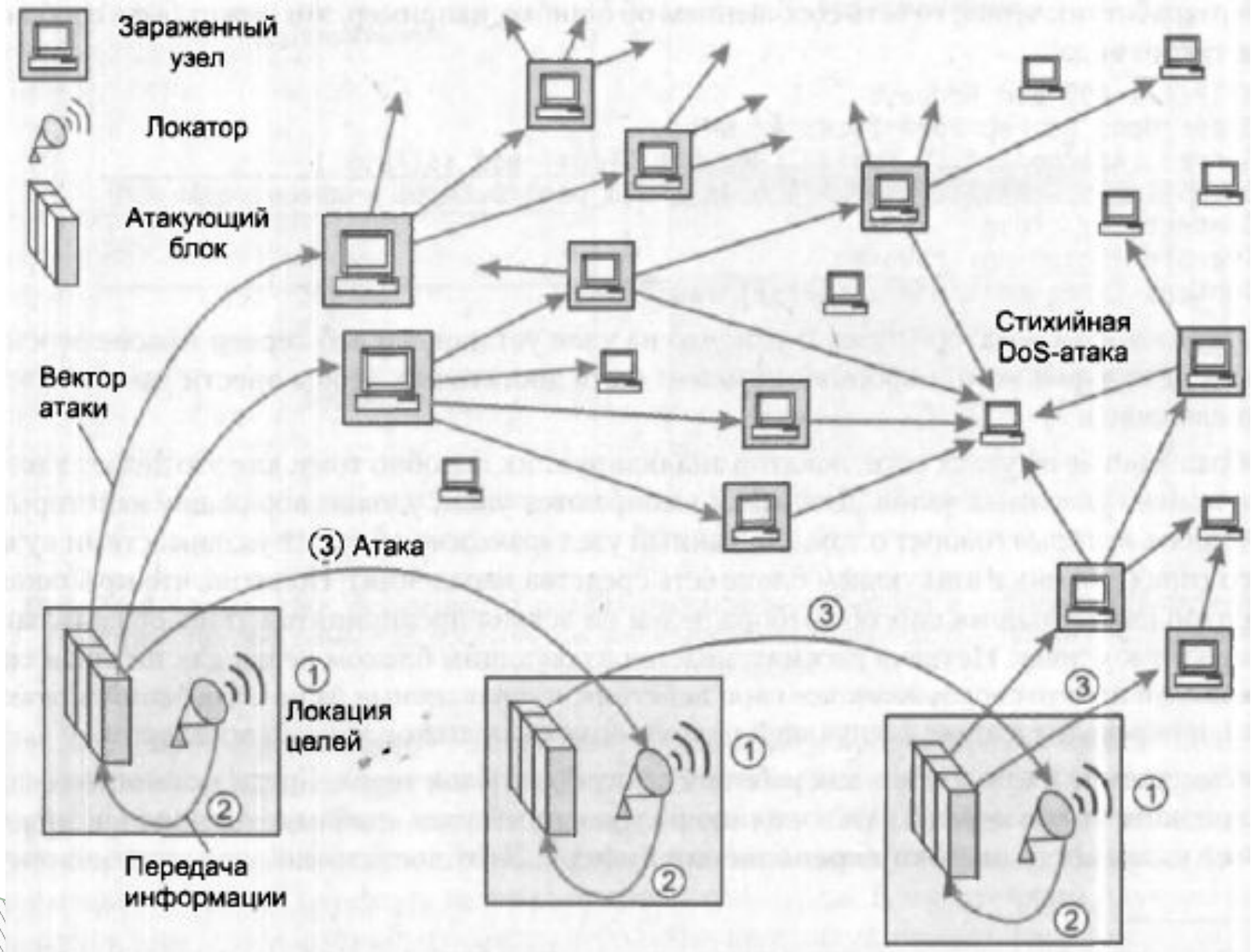
Сетевые черви-создание

- Если червь обладает возможностью повторного заражения, то число его копий растет лавинообразно, все более и более загружают процессор, захватываются новые области памяти, снижается пропускную способность сетевых соединений, пока, наконец, программы легальных пользователей не потеряют возможность выполняться.
- При создании типичного сетевого червя, прежде всего, определяет перечень сетевых уязвимостей, необходимых для проведения атак. Такими уязвимостями могут быть как известные, но не исправленные на некоторых компьютерах ошибки в программном обеспечении, так и пока неизвестные никому ошибки, которые обнаружил сам хакер. Чем шире перечень уязвимостей и чем более они распространены, тем больше узлов может быть поражено данным червем.
- Червь состоит из двух основных функциональных компонентов: атакующего блока и блока поиска целей.
  - **Атакующий блок** состоит из нескольких модулей **(векторов атаки),** каждый из которых рассчитан на поражение конкретного типа уязвимости. Этот блок открывает «входную дверь» атакуемого хоста и передает через нее свою копию.
  - **Блок поиска целей (локатор)** собирает информацию об узлах сети, а затем на основании этой информации определяет, какие из исследованных узлов обладают теми уязвимостями, для которых хакер имеет средства атаки.

Сетевые черви алгоритмы воздействия.

- Эти два функциональных блока являются *обязательными* и присутствуют в реализации любой программы-червя. Некоторые черви нагружены и другими вспомогательными функциями.
- Упрощенно жизненный цикл червя может быть описан рекурсивной процедурой, состоящей из циклического запуска локатора и атакующего блока на каждом из последующих заражаемых компьютеров (рис. 6-35.5).
- В начале каждого нового цикла червь, базирующийся на захваченном в результате предыдущей атаки компьютере, запускает локатор для поиска и формирования списка узлов-целей, пригодных для проведения каждой из специфических атак, а затем, используя средства атакующего блока, пытается эксплуатировать уязвимости узлов из этого списка. В результате успешной атаки червь копирует все свои программы на «новую территорию» и активирует локатор. После этого начинается новый цикл. На рисунке показано, как червь лавинообразно распространяется по сети. Заражение тысяч компьютеров может занять всего несколько минут. Некоторые виды червей не нападают на уже зараженные и/или подвергающиеся атаке в данный момент узлы. Если же такая проверка не предусмотрена в алгоритме работы червя, то в сети случайным образом могут возникать очаги стихийных DoS-атак.

Экспансия червя в сети



- **Рис. 6-35.5.** Экспансия червя в сети

Сетевые черви –модуль «локатор»

- Локатор идентифицирует цели по адресам электронной почты, IP-адресам, характеристикам установленных на хостах операционных систем, номерам портов, типам и версиям приложений.
- Локатор может получить нужную информации локально, на захваченном им в данный момент хосте прочитать файл, содержащий адресную книгу клиента электронной почты или путем зондирования сетевого окружения: таблицы конфигурационных параметров сетевых интерфейсов, ARP-таблицы и таблицы маршрутизации. Зная IP-конфигурацию хоста базирования и шлюзов, локатор достаточно просто может определить IP-адреса других узлов этой сети. Для идентификации узлов локатор может также использовать ICMP-сообщения или запросы ping, указывая в качестве адресов назначения все возможные IP-адреса. Для определения того, какие приложения работают на том или ином хосте, локатор сканирует различные *хорошо известные* номера TCP- и UDP-портов. Определив тип приложения, локатор пытается получить более детальные характеристики этого приложения.

Сетевые черви –модуль «локатор» пример поиска

- Например, пусть некоторая программа-червь имеет в своем арсенале средства для атаки на некоторые версии веб-сервера Apache. Для поиска потенциальных жертв локатор этого червя зондирует узлы сети, посылая умышленно ошибочные запросы к веб-серверу:
- GET / HTTP / 1 .l \ r \ n \ r \n
- Узел, на котором установлен сервер Apache, отвечает на такой запрос так, как и рассчитывал разработчик червя, то есть сообщением об ошибке, например, это может быть сообщение такого вида:
- HTTP/1.1 400 Bad Request
- Date: Mon, 23 Feb 2004 23:43:42 GMT
- Server: Apache/1.3.19 (UNIX) (Red-Hat/Linux) mod_ssl/2.8.1
- OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4p11 mod_perl/1,24_01
- Connection: close
- Transfer-Encoding: chunked
- Content-Type: text / html ; charset=iso-8859-l

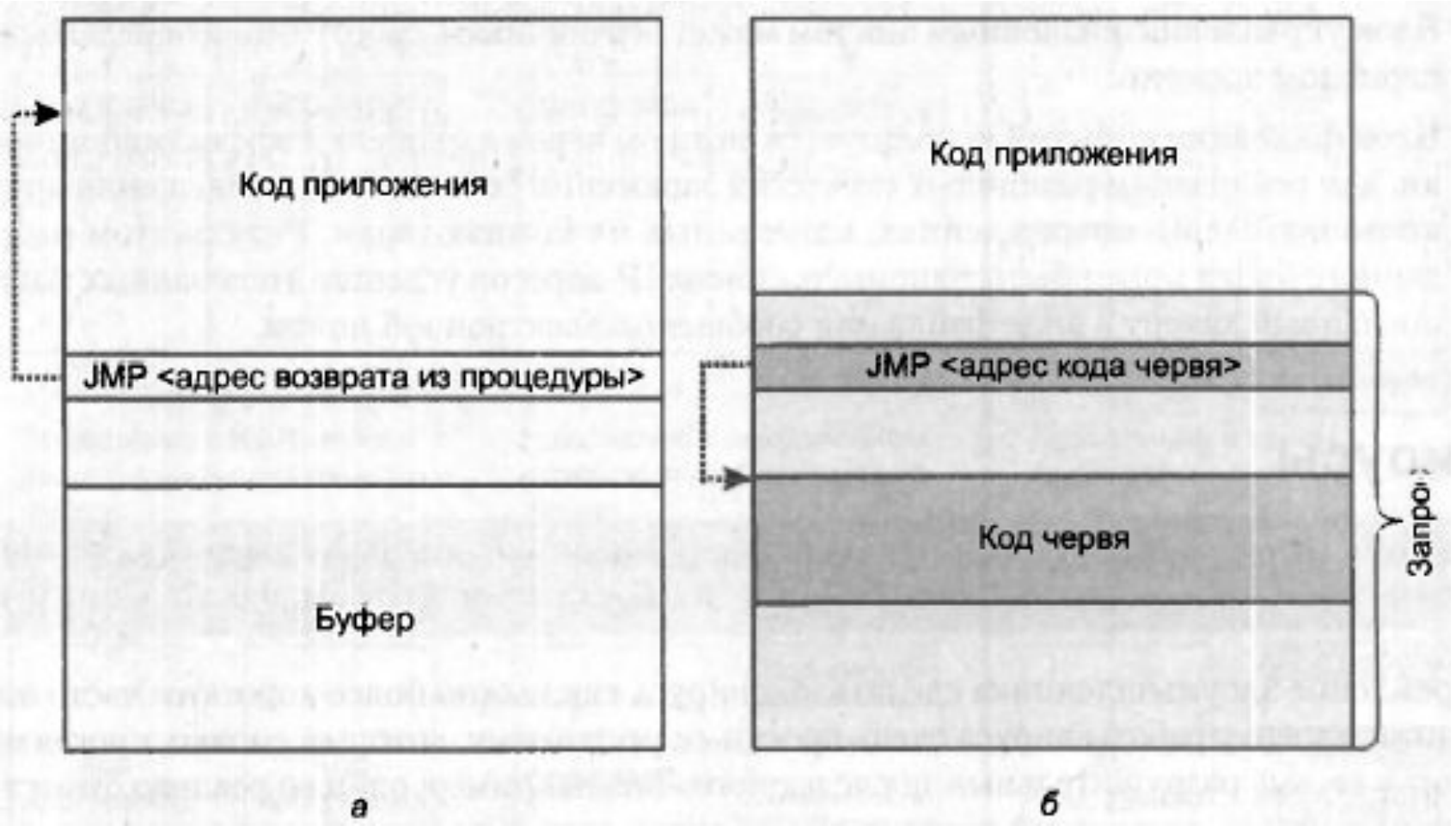
Сетевые черви –модуль «локатор» пример поиска

- Из этого ответа локатор узнает о том, что на узле установлен веб-сервер Apache версии 1.3.19. Для червя этой информации может быть достаточно, чтобы внести данный узел в число целей.
- Собрав данные об узлах сети, локатор анализирует их на предмет уязвимости. Для атаки выбираются узлы, удовлетворяющие некоторым условиям, а именно, что данный узел, *возможно,* обладает уязвимостями нужного типа (для них в атакующем блоке есть средства нападения). Понятно, что при таком «предположительном» способе отбора целей не всякая предпринятая атака обязательно приводит к успеху. Неудача рассматривается атакующим блоком червя как штатная ситуация, он просто сворачивает все свои действия, направленные на не поддавшийся атаке узел, и переходит к атаке следующей цели из списка, подготовленного локатором.
- Рассмотрим более подробно, как работает атакующий блок червя. Среди механизмов, позволяющих червю передать свою копию на удаленный узел, наиболее длинную историю имеет уязвимость **ошибки переполнения буфера.** Этот достаточно распространенный вид уязвимости связан с неправильной работой некоторых программ, когда у них переполняется буфер.

Сетевые черви – Атакующий блок

- При трансляции программ, написанных на многих языках программирования, в исполняемом (объектном) модуле в сегменте локальных переменных отводится место для буферов, в которые будут загружаться данные при выполнении процедур ввода. Например, в программе веб-сервера должен быть предусмотрен буфер для размещения запросов, поступающих от клиентов. Причем размер буфера должен быть равен максимально допустимой для данного протокола длине запроса. В том же сегменте локальных переменных транслятор размещает команду возврата из процедуры, которой будет передано управление при завершении процедуры (рис. 6-35.6, а).
- Для правильной работы программы очень важно, чтобы вводимые данные (в нашем примере — запрос клиента) всегда укладывались в границы отведенного для них буфера.
- В противном случае эти данные записываются поверх команды возврата из процедуры.
- А это, в свою очередь, означает, что процедура не сможет завершиться корректно: при передаче управления на адрес команды возврата процессор будет интерпретировать в качестве команды то значение из запроса, которое записано поверх команды возврата. Если такого рода переполнение возникло в результате случайной ошибки, то маловероятно, что значение, записанное поверх команды возврата, окажется каким-либо осмысленным кодом.
- Иное дело, если это переполнение было специально инициировано злоумышленником.

Схема атаки на уязвимость ошибки



- **Рис. 6-35.6.** Схема атаки на уязвимость ошибки переполнения буфера: а — структура адресного пространства программы до поступления злонамеренного запроса; б — после поступления злонамеренного запроса

Типы и примеры атак атакующий блок червя

- Злоумышленник конструирует запрос так, чтобы сервер прореагировал на него предсказуемым и желательным для хакера образом. Для этого хакер посылает нестандартный запрос, размер которого превышает размер буфера (рис. 6-35.6, Б). При этом среди данных запроса в том месте, которое приходится как раз на команду возврата, злоумышленник помещает команду перехода на вредоносный код червя. В простейшем случае таким вредоносным кодом может быть совсем небольшая программа, переданная в том же запросе.
- Итак, атакующий блок червя посылает некорректный запрос уязвимому серверу, его буфер переполняется, код команды возврата из процедуры замещается кодом команды передачи управления вредоносной программе, которая выполняет копирование всех оставшихся программных модулей червя на вновь освоенную территорию.
- Хотя рассмотренный подход применим к самым различным приложениям, для каждого типа приложений хакер должен сформировать специальный атакующий запрос, в котором *смещение кода команды передачи управления вредоносной программе точно соответствовало бы местоположению команды возврата в процедуру атакуемого приложения.* Именно поэтому для червя при проведении такого вида атак так важно получить информацию о типе и версиях программного обеспечения, установленного на узлах сети.

Блоки и модули сетевого червя

- Помимо локатора и атакующего блока червь может включать некоторые дополнительные функциональные компоненты.
- **Блок удаленного управления и коммуникаций** служит для передачи сетевым червям команд от их создателя, а также для взаимодействия червей между собой. Такая возможность позволяет хакеру координировать работу червей для организации распределенных атак отказа в обслуживании. Сетевые черви могут быть также использованы для организации параллельных вычислений при решении таких требующих большого объема вычислений задач, как, например, подбор секретного ключа шифрования или пароля.
- **Блок управления жизненным циклом** может ограничивать работу червя определенным периодом времени.
- **Блок фиксации событий** используется автором червя для оценки эффективности атаки, для реализации различных стратегий заражения сети или для оповещения других пользователей о повреждениях, нанесенных их компьютерам. Результатом работы данного блока может быть, например, список IP-адресов успешно атакованных машин, посланный хакеру в виде файла или сообщения электронной почты.

Вирусы

- **Вирус** (virus) — это вредоносный программный фрагмент, который может внедряться в другие файлы.
- Стремление злоумышленника сделать код вируса как можно более коротким часто ограничивает логику работы вируса очень простыми решениями, которые, однако, иногда приводят к весьма разрушительным последствиям. Так, например, один из реально существовавших вирусов, состоящий всего из 15 (!) байтов, записывал свою копию поверх других файлов в начало каждого сектора диска, в результате система очень быстро терпела крах.
- Некоторым утешением в таком и подобных ему случаях является то, что одновременно с крахом компьютера прекращает свое существование и вирус.
- Вирус может внедрять свои фрагменты в разные типы файлов, в том числе в файлы исполняемых программ (рис. 6-35.7). При этом возможны самые разные варианты: замещение кода, когда размер инфицированного файла не меняется, вставка вирусного кода целиком в начало или конец исходной программы, замена фрагментов программного кода фрагментами вируса с перестановкой замещенных фрагментов и без перестановки и т. д., и т. п.
- Более того, код вируса может быть зашифрован, чтобы затруднить его обнаружение антивирусными программами.

Вирусы

Рис. 6-35.7. Различные варианты расположения кода вируса в зараженных файлах

Вирусы

- Вирусы (так же как и троянские программы) не содержат в себе встроенного механизма активного распространения по сети, они способны размножаться своими силами только в *пределах одного компьютера.* Как правило, передача копии вируса на другой компьютер происходит с *участием пользователя.* Например, пользователь может записать файл, зараженный вирусом, на сетевой файловый сервер, и далее скопирован всеми пользователями, данного сервера. Пользователь может также передать другому пользователю съемный носитель с зараженным файлом или послать такой файл по электронной почте. То есть именно пользователь является главным звеном в цепочке распространения вируса за пределы своего компьютера. ***Последствий вирусного заражения*** зависит от того, какие вредоносные действия были запрограммированы в вирусе злоумышленником. Это могут быть мелкие, но раздражающие неудобства (замедление работы компьютера, уменьшение размеров доступной памяти, трата рабочего времени на переустановку приложений) или серьезные нарушения безопасности, такие как утечка конфиденциальных данных, разрушение системного программного обеспечения, частичная или полная потеря работоспособности компьютерной сети.

Шпионские программы

- ***Шпионские программы (spyware)*** — это такой тип вредоносных программ, которые тайно (как правило, удаленно) устанавливаются злоумышленниками на компьютеры ничего не подозревающих пользователей, чтобы отслеживать и фиксировать все их действия.
- В число таких действий может входить введение имени и пароля во время логического входа в систему, посещение тех или иных веб-сайтов, обмен информацией с внешними и внутренними пользователями сети и пр., и пр. Собранная информация пересылается злоумышленнику, который применяет ее в преступных целях.
- Заметим, что в качестве шпионских программ могут использоваться не только созданные специально для этих целей вредоносные программы, но и программы легального назначения. Так, опасным средством шпионажа могут стать легальные системы мониторинга сети, такие, например, как популярные сетевые мониторы Wireshark или Microsoft Network Monitor. Исходное назначение этих программ состоит в том, чтобы дать администратору сети возможность следить за сетевым трафиком, в частности захватывать пакеты, используя механизм фильтрации, просматривать их содержимое, собирать статистику по загрузке устройств.

Шпионские программы

- В руках же злоумышленника такая программа превращается в мощный инструмент «взлома» сети, который позволяет перехватывать пакеты с паролями и другой секретной информацией. Они также позволяют путем сканирования TCP- и UDP-портов определять типы приложений, работающих в сети, что является очень важной информацией для подготовки атаки.
- **ПРИМЕЧАНИЕ**
- Практически все сетевые мониторы построены в архитектуре клиент-сервер. Клиенты, обычно называемые агентами, захватывают и, если необходимо, фильтруют трафик, а затем передают его серверной части монитора для дальнейшей обработки. Серверная часть монитора может работать как в локальной сети, так и на удаленном компьютере, однако клиентские части всегда устанавливаются на компьютерах в тех сегментах сети, в которых протекает интересующий администратора (или злоумышленника) трафик. Необходимым условием для работы агентов монитора является установка сетевого адаптера компьютера, на котором запущен этот агент, в неразборчивый режим. Поэтому одним из способов, пресекающих несанкционированный захват и анализ сетевого трафика, является отслеживание всех интерфейсов сети, работающих в неразборчивом режиме приема.

Спам

- **Спам** — это атака, выполненная путем злоупотребления возможностями электронной почты.
- Учитывая ту важную роль, которую играет электронная почта в работе современных предприятий и организаций, можно понять, почему спам, дезорганизующий работу этой службы, стал рассматриваться в последние годы как одна из существенных угроз безопасности.
- 1 Программные системы, предназначенные для анализа сетевого трафика, называют также **снифферами** (sniffers от английского sniff — нюхать).
- 2 Спам получил свое название по имени реально существующих консервов Spam, которые стали темой одного из эпизодов популярного английского сериала. В этом эпизоде посетители кафе страдают оттого, что им постоянно навязывают блюда, в которых присутствуют эти консервы.
- Спам отнимает время и ресурсы на просмотр и удаление бесполезных сообщений, при этом ошибочно могут быть удалены письма с критически важной информацией, особенно велика вероятность этого при автоматической фильтрации писем.

Спам

- Посторонняя почта, которая нередко составляет 70 % получаемых сообщений, не только снижает эффективность работы предприятия, но и зачастую служит средством внедрения вредоносных программ. Кроме того, спам часто является элементом различных мошеннических схем, жертвами которых могут стать как отдельные сотрудники, так и предприятие в целом.
- Спамеры, то есть лица, рассылающие спам, используют для своих целей разнообразные и иногда весьма сложные методы и средства. Так, например, для пополнения баз данных адресов ими может выполняться автоматическое сканирование страниц Интернета, а для организации массовой рассылки они могут прибегать к распределенным атакам, когда зомбированные с помощью червей компьютеры бомбардируют спамом огромное число пользователей сети.
- **Список использованных источников**
- В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г