Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра компьютерных технологий

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Конспект лекций для студентов специальности
5В070400 – Вычислительная техника и программное обеспечение

Алматы 2014

СОСТАВИТЕЛИ: Тойгожинова А.Ж., Тергеусизова А.С. Безопасность компьютерных систем и сетей. Конспект лекций для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение. – Алматы: АУЭС, 2014. – 53 с.

Конспект лекций составлен согласно рабочей программе дисциплины Безопасность компьютерных систем и сетей. В данной работе рассмотрены основные протоколы безопасности, приведены уязвимости компьютерных сетей и проблемы безопасности протоколов TCP/IP. Рассмотрены процессы экранирования и принципы работы межсетевых экранов.

Конспект лекций предназначен для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение.

Табл. 7, библиогр. 29 назв.

Рецензент: кандидат физико-математических наук, доцент Шайхин Б.М.

Печатается по плану издания Некоммерческое Акционерное Общество «Алматинский университет энергетики и связи» на 2014 г.

© НАО «Алматинский университет энергетики и связи», 2014 г.

Введение

Компьютеры, сети, Интернет стали неотъемлемой частью нашей повседневной жизни. Наш быстроразвивающийся, насыщенный технологиями мир с каждым днем все больше становится зависимым от компьютерных технологий и сетей. Однако эта зависимость возникла не внезапно. С каждым годом финансирование компьютерных технологий значительно возрастало, и неудивительно, что эти технологии проникли практически во все сферы деятельности человека.

В настоящее время огромное количество сетей объединено посредством Интернет. Поэтому очевидно, что для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации, причем опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа.

Учитывая эти факты, можно с уверенностью сказать, что проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут финансовые убытки.

Помимо кражи информации, опасность могут представлять атаки типа «отказ в обслуживании» и кража услуг.

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в неё изменений неуполномоченными лицами, и сохранение тайны переписки электронной связи. Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, поэтому надежность работы компьютерных систем во многом опирается на меры самозащиты.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

В данном конспекте лекций отражены основные принципы обеспечения безопасности компьютерных систем и сетей.

Лекция №1. Стандарты и технические спецификации в области информационной безопасности

Цель лекций: ознакомление с оценочными стандартами и техническими спецификациями в области информационной безопасности.

Бывают *оценочные стандарты,* направленные на классификацию информационных систем и средств защиты по требованиям безопасности и *технические спецификации,* регламентирующие различные аспекты реализации средств защиты.

«Оранжевая книга» как оценочный стандарт.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «*Критерии оценки доверенных компьютерных систем»*. Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 года. Из его названия следует, что речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

«Оранжевая книга» дает *понятие безопасной системы*, которая «управляет, с помощью соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию». Очевидно, что абсолютно безопасных систем не существует, поэтому есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В «Оранжевой книге» *доверенная система* определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

В рассматриваемых критериях безопасность и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности «Оранжевая книга» не затрагивает.

Степень доверия оценивается по двум основным критериям:

Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это *активный аспект защиты*, включающий в себя анализ возможных угроз и выбор мер противодействия.

Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может

проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Из пассивных аспектов защиты в «Оранжевой книге» рассматривается два вида гарантированности - операционная и технологическая.

Операционная гарантированность относится к архитектурным и реализационным аспектам системы, технологическая - к методам построения и сопровождения. Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Технологическая гарантированность охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные «закладки».

Важным средством обеспечения безопасности является механизм протоколирования. Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор. Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Лекция №2. Компьютерные атаки и технологии их обнаружения

Цель лекций: ознакомить студентов с моделями и этапами сетевых атак, рассмотреть принципы реализации атак, а также классификацию атак. Приведены средства обнаружения компьютерных атак.

Атакой на информационную систему называются преднамеренные действия злоумышленника, использующие уязвимости информационной системы и приводящие к нарушению доступности, целостности и конфиденциальности обрабатываемой информации.

Модели атак.

Традиционная модель атаки строится по принципу «один к одному» (рисунок 2.1) или «один ко многим» (рисунок 2.2), т.е. атака исходит о одного источника.

Рисунок 2.1 - Отношение "один к одному"

Рисунок 2.2 - Отношение «один ко многим»

В модели распределенной атаки используются иные принципы. В отличие от традиционной модели в распределенной модели используются отношения «многие к одному» (рисунок 2.3) и «многие ко многим» (рисунок 2.4).

Рисунок 2.3 – Отношение «многие к одному»

Распределенные атаки основаны на «классических» атаках типа «отказ в обслуживании», а точнее на их подмножестве, известном как Flood-атаки или Storm-атаки (указанные термины можно перевести как «шторм», «наводнение» или «лавина»). Смысл данных атак заключается в посылке большого количества пакетов на атакуемый узел. Атакуемый узел может выйти из строя, поскольку он «захлебнется» в лавине посылаемых пакетов и не сможет обрабатывать запросы авторизованных пользователей. По такому принципу работают атаки SYN-Flood, Smurf, UDP Flood и т.д. Однако в том

Рисунок 2.4 - Отношение «многие ко многим»

случае, если пропускная способность канала до атакуемого узла превышает пропускную способность атакующего или атакуемый узел некорректно сконфигурирован, то к «успеху» такая атака не приведет. Например, с помощью этих атак бесполезно пытаться нарушить работоспособность своего провайдера. Но распределенная атака происходит уже не из одной точки Internet, а сразу из нескольких, что приводит к резкому возрастанию трафика и выведению атакуемого узла из строя.

Лекция №3. Этапы реализации атак

Можно выделить следующие этапы реализации атаки:
- предварительные действия перед атакой или "сбор информации";
- собственно "реализация атаки";
- завершение атаки.

Обычно, когда говорят об атаке, то подразумевают именно второй этап, забывая о первом и последнем. Сбор информации и завершение атаки ("заметание следов") в свою очередь также могут являться атакой и могут быть разделены на три этапа (рисунок 2.5).

Рисунок 2.5 - Этапы реализации атаки

Сбор информации - это основной этап реализации атаки. Именно на данном этапе эффективность работы злоумышленника является залогом «успешности» атаки. Сначала выбирается цель атаки и собирается информация о ней (тип и версия операционной системы, открытые порты и

запущенные сетевые сервисы, установленное системное и прикладное программное обеспечение и его конфигурация и т.д.). Затем идентифицируются наиболее уязвимые места атакуемой системы, воздействие на которые приводит к нужному злоумышленнику результату. Злоумышленник пытается выявить все каналы взаимодействия цели атаки с другими узлами. Это позволит не только выбрать тип реализуемой атаки, но и источник ее реализации.

Традиционные средства защиты такие, как межсетевые экраны или механизмы фильтрации в маршрутизаторах, вступают в действие лишь на втором этапе реализации атаки, совершенно «забывая» о первом и третьем. Это приводит к тому, что зачастую совершаемую атаку очень трудно остановить даже при наличии мощных и дорогих средств защиты. Пример тому - распределенные атаки. Логично было бы, чтобы средства защиты начинали работать еще на первом этапе, т.е. предотвращали бы возможность сбора информации об атакуемой системе. Это позволило бы, если и не полностью предотвратить атаку, то хотя бы существенно усложнить работу злоумышленника. Традиционные средства также не позволяют обнаружить уже совершенные атаки и оценить ущерб после их реализации, т.е. не работают на третьем этапе реализации атаки. Следовательно, невозможно определить меры по предотвращению таких атак впредь.

В зависимости от желаемого результата нарушитель концентрируется на том или ином этапе реализации атаки.

Например:

- для отказа в обслуживании подробно анализируется атакуемая сеть, в ней выискиваются лазейки и слабые места;

- для хищения информации основное внимание уделяется незаметному проникновению на атакуемые узлы при помощи обнаруженных ранее уязвимостей.

Рассмотрим основные механизмы реализации атак. Это необходимо для понимания методов обнаружения этих атак. Кроме того, понимание принципов действий злоумышленников - залог успешной обороны сети.

1. Сбор информации.

Первый этап реализации атак - это сбор информации об атакуемой системе или узле. Он включает такие действия как определение сетевой топологии, типа и версии операционной системы атакуемого узла, а также доступных сетевых и иных сервисов и т.п. Эти действия реализуются различными методами.

Изучение окружения.

На этом этапе нападающий исследует сетевое окружение вокруг предполагаемой цели атаки. К таким областям, например, относятся узлы Internet-провайдера «жертвы» или узлы удаленного офиса атакуемой компании. На этом этапе злоумышленник может пытаться определить адреса «доверенных» систем (например, сеть партнера) и узлов, которые напрямую соединены с целью атаки (например, маршрутизатор ISP) и т.д. Такие действия достаточно трудно обнаружить, поскольку они выполняются в течение достаточно длительного периода времени и снаружи области,

контролируемой средствами защиты (межсетевыми экранами, системами обнаружения атак и т.п.).

Идентификация топологии сети.

Существует два основных метода определения топологии сети, используемых злоумышленниками:

- изменение TTL (TTL modulation);
- запись маршрута (record route).

По первому методу работают программы traceroute для Unix и tracert для Windows. Они используют поле Time to Live («время жизни») в заголовке IP-пакета, которое изменяется в зависимости от числа пройденных сетевым пакетом маршрутизаторов. Для записи маршрута ICMP-пакета может быть использована утилита ping . Зачастую сетевую топологию можно выяснить при помощи протокола SNMP, установленного на многих сетевых устройствах, защита которых неверно сконфигурирована. При помощи протокола RIP можно попытаться получить информацию о таблице маршрутизации в сети и т.д.

Идентификация узлов.

Идентификация узла, как правило, осуществляется путем посылки при помощи утилиты ping команды ECHO_REQUEST протокола ICMP. Ответное сообщение ECHO_REPLY говорит о том, что узел доступен. Существуют свободно распространяемые программы, которые автоматизируют и ускоряют процесс параллельной идентификации большого числа узлов, например, fping или nmap. Опасность данного метода в том, что стандартными средствами узла запросы ECHO_REQUEST не фиксируются. Для этого необходимо применять средства анализа трафика, межсетевые экраны или системы обнаружения атак.

Это самый простой метод идентификации узлов. Однако он имеет два недостатка.

Многие сетевые устройства и программы блокируют ICMP-пакеты и не пропускают их во внутреннюю сеть (или наоборот не пропускают их наружу). С другой стороны, блокировка ICMP-пакета говорит злоумышленнику о наличии «первой линии обороны» - маршрутизаторов, межсетевых экранов и т.д.

Использование ICMP-запросов позволяет с легкостью обнаружить их источник, что, разумеется, не может входить в задачу злоумышленника.

Существует еще один метод идентификации узлов - использование «смешанного» режима сетевой карты, который позволяет определить различные узлы в сегменте сети. Но он не применим в тех случаях, в которых трафик сегмента сети недоступен нападающему со своего узла, т.е. этот метод применим только в локальных сетях. Другим способом идентификации узлов сети является так называемая разведка DNS, которая позволяет идентифицировать узлы корпоративной сети при помощи обращения к серверу службы имен.

Идентификация сервисов или сканирование портов.

Идентификация сервисов, как правило, осуществляется путем обнаружения открытых портов (port scanning). Такие порты очень часто

связаны с сервисами, основанными на протоколах TCP или UDP. Например: открытый 80-й порт подразумевает наличие Web-сервера, 25-й порт - почтового SMTP-сервера.

Для идентификации сервисов и сканирования портов могут быть использованы различные программы, в т.ч. и свободно распространяемые. Например, nmap или netcat.

Идентификация операционной системы.

Основной механизм удаленного определения ОС - анализ ответов на запросы, учитывающие различные реализации TCP/IP-стека в различных операционных системах. В каждой ОС по-своему реализован стек протоколов TCP/IP, что позволяет при помощи специальных запросов и ответов на них определить, какая ОС установлена на удаленном узле.

Другой, менее эффективный и крайне ограниченный, способ идентификации ОС узлов - анализ сетевых сервисов, обнаруженных на предыдущем этапе.

Определение роли узла.

Предпоследним шагом на этапе сбора информации об атакуемом узле является определение его роли, например, выполнении функций межсетевого экрана или Web-сервера. Выполняется этот шаг на основе уже собранной информации об активных сервисах, именах узлов, топологии сети и т.п.

Определение уязвимостей узла.

Последний шаг - поиск уязвимостей. На этом шаге злоумышленник при помощи различных автоматизированных средств или вручную определяет уязвимости, которые могут быть использованы для реализации атаки. В качестве таких автоматизированных средств могут быть использованы ShadowSecurityScanner, nmap, Retina и т.д.

2. Реализация атаки.

С этого момента начинается попытка доступа к атакуемому узлу. При этом доступ может быть как непосредственный, т.е. проникновение на узел, так и опосредованный, например, при реализации атаки типа «отказ в обслуживании». Реализация атак в случае непосредственного доступа также может быть разделена на два этапа:

- проникновение;
- установление контроля.

Проникновение,

Проникновение подразумевает под собой преодоление средств защиты периметра (например, межсетевого экрана). Реализовываться это может быть различными путями. Например, использование уязвимости сервиса компьютера, «смотрящего» наружу или путем передачи враждебного содержания по электронной почте (макровирусы) или через апплеты Java. Такое содержание может использовать так называемые «туннели» в межсетевом экране (не путать с туннелями VPN), через которые затем и проникает злоумышленник. К этому же этапу можно отнести подбор пароля администратора или иного пользователя при помощи специализированной утилиты.

Установление контроля.

После проникновения злоумышленник устанавливает контроль над атакуемым узлом. Это может быть осуществлено путем внедрения программы типа «троянский конь». После установки контроля над нужным узлом и «заметания» следов, злоумышленник может осуществлять все необходимые несанкционированные действия дистанционно без ведома владельца атакованного компьютера. При этом установление контроля над узлом корпоративной сети должно сохраняться и после перезагрузки операционной системы. Это может быть реализовано путем замены одного из загрузочных файлов или вставка ссылки на враждебный код в файлы автозагрузки или системный реестр.

Цели реализации атак.

Необходимо отметить, что злоумышленник на втором этапе может преследовать две цели. Во-первых, получение несанкционированного доступа к самому узлу и содержащейся на нем информации. Во-вторых, получение несанкционированного доступа к узлу для осуществления дальнейших атак на другие узлы. Первая цель, как правило, осуществляется только после реализации второй. То есть, сначала злоумышленник создает себе базу для дальнейших атак и только после этого проникает на другие узлы. Это необходимо для того, чтобы скрыть или существенно затруднить нахождение источника атаки.

3. Завершение атаки.

Этапом завершения атаки является «заметание следов» со стороны злоумышленника. Обычно это реализуется путем удаления соответствующих записей из журналов регистрации узла и других действий, возвращающих атакованную систему в исходное, «предатакованное» состояние.

Классификация атак.

Существуют различные типа классификации атак. Например, деление на пассивные и активные, внешние и внутренние, умышленные и неумышленные. Однако, чтобы не запутаться большим разнообразием классификаций, мало применимыми на практике, предлагается более «жизненная» классификация:

Удаленное проникновение (remote penetration). Атаки, которые позволяют реализовать удаленное управление компьютером через сеть. Например, NetBus или BackOrifice.

Локальное проникновение (local penetration). Атака, которая приводит к получению несанкционированного доступа к узлу, на котором она запущена. Например, GetAdmin.

Удаленный отказ в обслуживании (remote denial of service). Атаки, которые позволяют нарушить функционирование или перегрузить компьютер через Internet. Например, Teardrop или trin00.

Локальный отказ в обслуживании (local denial of service). Атаки, которые позволяют нарушить функционирование или перегрузить компьютер, на котором они реализуются. Примером такой атаки является «враждебный» апплет, который загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений.

Сетевые сканеры (network scanners). Программы, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки. Например, система nmap.

Сканеры уязвимостей (vulnerability scanners). Программы, которые ищут уязвимости на узлах сети и которые могут быть использованы для реализации атак. Например, система SATAN или ShadowSecurityScanner.

Взломщики паролей (password crackers). Программы, которые «подбирают» пароли пользователей. Например, L0phtCrack для Windows или Crack для Unix.

Анализаторы протоколов (sniffers). Программы, которые «прослушивают» сетевой трафик. При помощи этих программ можно автоматически искать такую информацию, как идентификаторы и пароли пользователей, информацию о кредитных картах и т.д. Например, Microsoft Network Monitor, NetXRay компании Network Associates или LanExplorer.

Компания Internet Security Systems, Inc. еще больше сократила число возможных категорий, доведя их до 5:

- сбор информации (Information gathering);
- попытки несанкционированного доступа (Unauthorized access attempts);
- отказ в обслуживании (Denial of service);
- подозрительная активность (Suspicious activity);
- системные атаки (System attack).

Первые 4 категории относятся к удаленным атакам, а последняя - к локальным, реализуемом на атакуемом узле. Можно заметить, что в данную классификацию не попал целый класс так называемых «пассивных» атак («прослушивание» трафика, «ложный DNS-сервер», «подмена ARP-сервера» и т.п.).

Средства обнаружения компьютерных атак.

Технология обнаружения атак должна решать следующие задачи:

Распознавание известных атак и предупреждение о них соответствующего персонала.

«Понимание» зачастую непонятных источников информации об атаках.

Освобождение или снижение нагрузки на персонал, отвечающий за безопасность, от текущих рутинных операций по контролю за пользователями, системами и сетями, являющимися компонентами корпоративной сети.

Возможность управления средствами защиты не-экспертами в области безопасности.

Контроль всех действий субъектов корпоративной сети (пользователей, программ, процессов и т.д.).

Контроль электронной почты. Системы обнаружения атак могут использоваться для контроля неблагонадежных сотрудников, использующих электронную почту для выполнения задач, не входящих в их функциональные обязанности, например, рассылка резюме.

Лучшее использование времени и опыта специалистов в области информационной безопасности заключается в обнаружении и устранении причин реализации атак, скорее чем, в обнаружении самих атак. Устранив

причины возникновения атак, т.е. обнаружив и устранив уязвимости, администратор тем самым устраняет и сам факт потенциальной реализации атак. Иначе атака будет повторяться раз за разом, постоянно требуя усилий и внимания администратора.

Классификация систем обнаружения атак

Существует большое число различных классификаций систем обнаружения атак, однако самой распространенной является классификация по принципу реализации:

- *host-based,* то есть обнаруживающие атаки, направленные на конкретный узел сети;
- *network-based,* то есть обнаруживающие атаки, направленные на всю сеть или сегмент сети.

Системы обнаружения атак, контролирующие отдельный компьютер, как правило, собирают и анализируют информацию из журналов регистрации операционной системы и различных приложений.

Системы обнаружения атак уровня сети собирают информацию из самой сети, то есть из сетевого трафика.

Обнаружение атак требует выполнения одного из двух условий - или понимания ожидаемого поведения контролируемого объекта системы или знания всех возможных атак и их модификаций. В первом случае используется технология обнаружения аномального поведения, а во втором случае - технология обнаружения злоумышленного поведения или злоупотреблений. Вторая технология заключается в описании атаки в виде шаблона или сигнатуры и поиска данного шаблона в контролируемом пространстве (например, сетевом трафике или журнале регистрации). Эта технология очень похожа на обнаружение вирусов (антивирусные системы являются ярким примером системы обнаружения атак), т.е. система может обнаружить все известные атаки, но она мало приспособлена для обнаружения новых, еще неизвестных, атак. Подход, реализованный в таких системах, очень прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак.

Лекция №4. Криптографические средства защиты компьютерных сетей

Цель лекций: изучить криптографические методы защиты информации в компьютерных сетях.

Криптография - это дисциплина, изучающая способы защиты процессов информационного взаимодействия от целенаправленных попыток отклонить их от условий нормального протекания, основанные на криптографических преобразованиях, то есть преобразованиях данных по секретным алгоритмам. Важнейшей задачей криптографии является защита передаваемых по каналам связи или хранящихся в системах обработки информации данных от несанкционированного ознакомления с ними и от преднамеренного их искажения. Криптография решает указанную задачу посредством шифрования

защищаемых данных, что предполагает использование двух следующих взаимно обратных преобразований - зашифрования и расшифрования.

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Секретность второго из них делает данные недоступными для несанкционированного ознакомления, а секретность первого делает невозможным навязывание ложных данных. Получение открытых данных по зашифрованным без знания алгоритма расшифрования называется дешифрованием.

Второе условие, которому должен удовлетворять шифр, следующее: он должен шифровать данные, то есть делать их непонятными для непосвященного.

Другими словами, не должно существовать легко прослеживаемых связей между исходными и зашифрованными данными. Кроме того, шифр должен быть криптостойким, то есть устойчивым к попыткам дешифрования сообщений.

Диффузия: каждый бит незашифрованного текста должен влиять на каждый бит зашифрованного текста. Распространение одного незашифрованного бита на большое количество зашифрованных битов скрывает статистическую структуру незашифрованного текста. Определить, как статистические характеристики зашифрованного текста зависят от статистических характеристик незашифрованного текста, должно быть непросто.

Несмотря на почтенный возраст криптографии, до сих пор не разработано единой четкой классификационной схемы, в которую бы укладывались все существующие на сегодняшний день алгоритмы. Существует три схемы классификации, основанные на различных характерных признаках, поэтому один и тот же алгоритм входит сразу в три группы.

По принципу действия все криптоалгоритмы делятся на три большие группы:

1) Тайнопись. Ее принцип очень прост. Отправитель преобразовывает информацию по определенному алгоритму. После этого она представляет собой набор беспорядочных данных. О том, какие преобразования нужно совершить, чтобы получить информацию в первозданном виде, знает только ее получатель. То есть сам алгоритм хранится в тайне. Если же злоумышленник сможет его получить, он будет иметь свободный доступ ко всем данным, зашифрованным с его помощью. Тайнопись - самая старая группа криптографических алгоритмов.

2) Симметричные криптоалгоритмы. В отличие от тайнописи, они сами по себе не являются секретными. В процессе кодирования данных симметричные криптоалгоритмы используют специальный ключ (блок информации). Он нужен как для шифрования, так и для дешифрования. А поэтому доступ к закодированной информации имеет ее владелец и люди, которые имеют ключ.

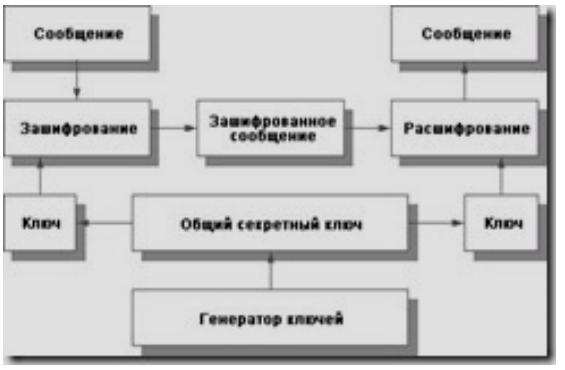

Рисунок 3.1 - Схема работы симметричного криптоалгоритма

3) Асимметричные криптоалгоритмы, называемые также алгоритмами с открытым или публичным ключом. В них, как и в предыдущем случае, используется шифрование с ключом. В асимметричных алгоритмах используется не один, а два различных ключа. Первый ключ - закрытый. Он является секретным, его должен знать только владелец. Второй ключ - открытый. Обычно он доступен для любых людей, с которыми владелец обменивается информацией. Причем получение его злоумышленниками не уменьшает степень защиты информации. Принцип действия асимметричных алгоритмов следующий. Любой человек может зашифровать данные с помощью открытого ключа другого пользователя. Расшифровать же их может только получатель с использованием закрытого ключа. Возможна и обратная процедура. Зашифрованная с помощью своего закрытого ключа информация может быть расшифрована только с использованием открытого ключа этого же человека. Используется она для реализации цифровой подписи.

Для целей конфиденциальности схема обмена информацией такова:

- получатель вычисляет свою пару ключей - открытый и закрытый ключи, закрытый ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);
- отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;
- получатель получает сообщение и расшифровывает его, используя свой закрытый ключ.

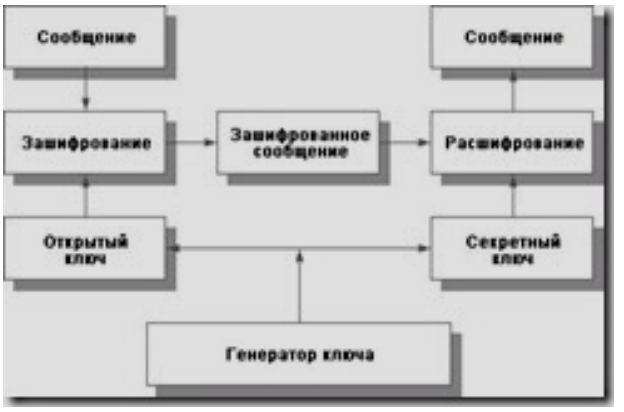

Рисунок 3.2 - Схема работы асимметричного криптоалгоритма для целей конфиденциальности

Сравнение симметричных и асимметричных алгоритмов шифрования.

В асимметричных системах необходимо применять длинные ключи (512 битов и больше). Длинный ключ резко увеличивает время шифрования. Кроме того, генерация ключей весьма длительна. Зато распределять ключи можно по незащищенным каналам.

В симметричных алгоритмах используют более короткие ключи, т. е. шифрование происходит быстрее. Но в таких системах имеется сложность распределения ключей, поэтому при проектировании защищенной системы часто применяют и симметричные, и асимметричные алгоритмы. Так как система с открытыми ключами позволяет распределять ключи и в симметричных системах, можно объединить в системе передачи защищенной информации асимметричный и симметричный алгоритмы шифрования. С помощью первого рассылать ключи, вторым - шифровать передаваемую информацию.

Обмен информацией можно осуществлять следующим образом:

- получатель вычисляет открытый и закрытый ключи, закрытый ключ хранит в тайне, открытый же делает доступным;
- отправитель, используя открытый ключ получателя, зашифровывает сеансовый ключ (секретный ключ симметричного алгоритма), который пересылается получателю по незащищенному каналу;
- получатель получает сеансовый ключ и расшифровывает его, используя свой закрытый ключ;
- отправитель зашифровывает сообщение сеансовым ключом и пересылает получателю;
- получатель получает сообщение и расшифровывает его сеансовым ключом.

По характеру воздействия на шифруемую информацию криптоалгоритмы делятся также на три группы:

1) Шифры перестановки. К первой относятся те из них, которые не меняют исходные данные, а всего лишь переставляют их части с места на место. Например, используя определенный алгоритм, текст можно "раскидать" по буквам. После этого он станет совершенно "неудобочитаемым". Для его дешифрования достаточно будет вернуть все знаки на свои места. Сегодня перестановочные криптографические алгоритмы практически не используются, так как они абсолютно непригодны для шифрования потоков информации при ее передаче и по надежности уступают другим криптографическим системам.

2) Шифры замены. Алгоритмы, относящиеся ко второй группе, основаны на характере воздействия на шифруемую информацию, называются подстановочными. Они меняют исходные данные, полностью заменяя определенные блоки данных другими. По надежности такие системы превосходят перестановочные.

3) К третьей группе относятся смешанные системы, в которых блоки информации сначала заменяются по определенным законам на другие, а потом перемешиваются. Это существенно замедляет процесс шифрования, однако обеспечивают большую степень защиты данных.

Лекция №5. Вредоносное программное обеспечение (вирусы)

Цель лекций: ознакомить студентов с разновидностями вредоносного программного обеспечения, программ-шпионов, техник их действия и распространения.

Считается, что термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Однако строгого определения, что же такое компьютерный вирус, так и не дано. Основная трудность, возникающая при попытках дать это определение, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и проч.) либо присущи другим программам, которые никак вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения). Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательным (необходимым) свойством вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Однако данное условие не является достаточным. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Вирус обычно имеет те же права доступа к сетевым ресурсам, что и пользователь, на компьютере которого находится этот вирус.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- заражаемая операционная система;
- особенности алгоритма работы;
- деструктивные возможности.

По среде обитания вирусы бывают:

- файловые;
- загрузочные;
- макро;
- сетевые.

Рисунок 4.1 - Распространение вируса по компьютерной сети

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, вывести из строя оборудование.

Среди особенностей алгоритма работы вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- метаморфичность.

Под термином «резидентность» (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Резидентные копии вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы.

Нерезидентные вирусы активны непродолжительное время — только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Первые антивирусные программы искали вирусы, сравнивая содержимое файлов и секторов диска с характерными фрагментами вирусов (с

сигнатурами вирусов). Именно эти фрагменты хранились в вирусных базах данных антивирусных программ.

Чтобы исключить обнаружение изделий, разработчики компьютерных вирусов стали применять шифрование вирусного кода. Шифрующийся вирус — это вирус, который при заражении новых файлов и системных областей диска шифрует собственный код, пользуясь для этого случайными паролями (ключами). Когда вирус получает управление, он расшифровывает свой собственный код и передает ему управление.

Современные антивирусы умеют расшифровывать код вируса, поэтому шифрующиеся вирусы могут быть эффективно обнаружены и уничтожены. Дальнейшее совершенствование шифрующихся вирусов было направлено на затруднение их обнаружения. С этой целью были разработаны так называемые полиморфные вирусы.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключем и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса.

Полиморфные генераторы.

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Метаморфные вирусы.

Метаморфные вирусы, так же изменяют свой код, но не используют алгоритмы шифрования. Различие проявляется в виде изменений внутри кода вируса. Существует несколько технологий, позволяющих с успехом реализовывать данную методику.

Одна из этих технологий трансформации, используемая метамофными программами основана на вставке и удалении «мусора» внутри кода. Эти инструкции не влияют на работу вируса, но занимают некоторое количество места и усложняют анализ больших участков кода.

Другая технология – изменение базовых инструкций на уровне кода. Это означает переключение между несколькими отличающимися кодами, которые выполняют одну и ту же функцию.

Загрузочные вирусы.

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера - после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса.

Существует несколько вариантов размещения на диске первоначального загрузочного сектора и продолжения вируса: в сектора свободных кластеров логического диска, в неиспользуемые или редко используемые системные сектора, в сектора, расположенные за пределами диска.

Макро-вирусы.

Макро-вирусы являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word и Excel.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макро-языка с возможностями:

- привязки программы на макро-языке к конкретному файлу;
- копирования макро-программ из одного файла в другой;
- возможность получения управления макро-программой без вмешательства пользователя (автоматические или стандартные макросы).

Данные особенности макро-языков предназначены для автоматической обработки данных в больших организациях или в глобальных сетях и позволяют организовать автоматизированный документооборот.

Лекция №6. Сетевые вирусы

К ним относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию и захватить управление. Для внедрения в заражаемую систему червь может использовать различные механизмы: дыры, слабые пароли, уязвимости базовых и прикладных протоколов, открытые системы и человеческий фактор.

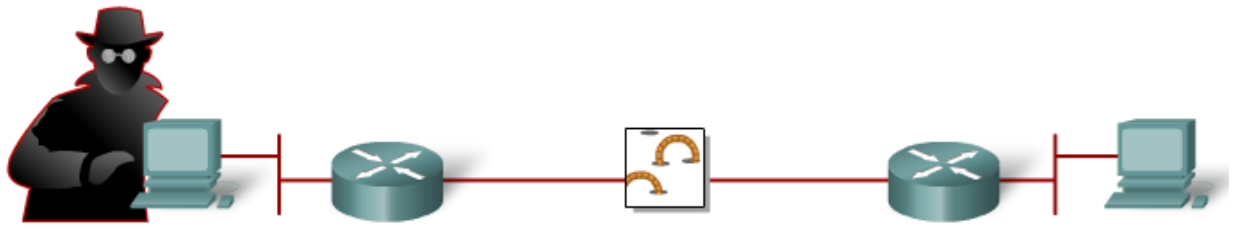

Рисунок 4.2 – Распространение сетевых вирусов (сетевые черви) по сети

Почтовые вирусы.

Почтовый вирус использует для своего распространения каналы электронной почты. Заражение почтовым вирусом происходит в результате действий пользователей, просматривающих почту, а также из-за ошибок в почтовых программах и операционных системах.

Вирусы для пиринговых сетей.

В современном Интернете имеется большое количество сетей, предназначенных для обмена файлами без применения централизованного сервера. Эти сети позволяют пользователям Интернета свободно обмениваться музыкальными файлами, программами и другой информацией. Эти сети часто называются файлообменными или пиринговыми. Последнее из этих названий происходит от названия применяемого в таких сетях способа обмена данными узел-узел (Peer-To-Peer). Для пиринговых сетей разработчиками вредоносных программ были созданы специальные вирусы, называемые вирусами для пиринговых сетей:

Вирус пиринговых сетей — это вредоносная программа, специально предназначенная для систем обмена файлами между компьютерами пользователей Интернета, такими как Windows Messenger, ICQ и т.д. Чтобы такой вирус попал на компьютер пользователя пиринговой сети, пользователю требуется выполнить какое либо действие, например, загрузить и запустить на выполнение файл.

Файловые вирусы.

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо ОС. Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. По способу заражения файлов вирусы делятся на «overwriting», паразитические («parasitic»), компаньон-вирусы («companion»), вирусы-черви.

Троянской программой (троянцем, или троянским конем) называется:

- программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;

- программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Таким образом, троянской можно считать любую программу, которая втайне от пользователя выполняет какие-то нежелательные (неожидаемые) для него действия. Эти действия могут быть любыми — от определения регистрационных номеров программного обеспечения, установленного на компьютере, до составления списка каталогов на его жестком диске. А сама троянская программа может маскироваться под текстовый редактор, под сетевую утилиту или любую программу, которую пользователь пожелает установить на свой компьютер.

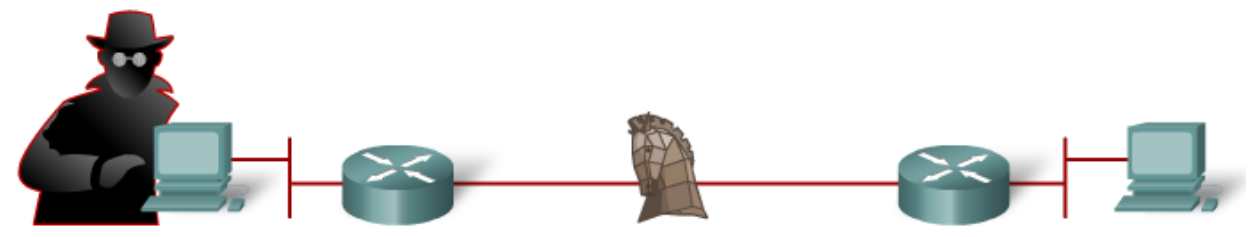

Рисунок 4.3 – Заражение компьютерной сети троянской программой

На сегодня известны троянские объекты следующих типов:

- троянские программы;
- троянские Web-сайты;
- троянские сообщения электронной почты.

Троянским называется такой Web-сайт, при посещении которого на компьютер пользователя незаметно устанавливаются вредоносные программные компоненты. Сообщения электронной почты могут использоваться для переноса вредоносных программных объектов. Такие объекты присоединяются к телу сообщения в виде файлов, или встраиваются непосредственно в текст сообщения, имеющего формат HTML. Внешне сообщение электронной почты, содержащее в том или ином виде вредоносный программный код, может выглядеть как обычное, информационное. Однако стоит открыть такое сообщение для просмотра, и вредоносный код получит управление.

Большинство троянских программ предназначено для сбора конфиденциальной информации. Остальные троянцы создаются для причинения прямого ущерба компьютерной системе, приводя ее в неработоспособное состояние.

Чтобы программная закладка могла произвести какие-либо действия по отношению к другим программам или по отношению к данным, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. Это возможно только при одновременном соблюдении следующих условий:

- программная закладка должна попасть в оперативную память компьютера (если закладка относится к первому типу, то она должна быть загружена до начала работы другой программы, которая является целью воздействия закладки, или во время работы этой программы);
- работа закладки, находящейся в оперативной памяти, начинается при выполнении ряда условий, которые называются активизирующими.

Утилиты скрытого администрирования (backdoor).

Троянские кони этого класса по своей сути является достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на троянца может отсутствовать в списке активных приложений. В результате "пользователь" этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Функции Backdoor могут быть заложены в программу ее разработчиком, например, с целью получения в дальнейшем несанкционированного доступа к функциям программы или ко всей компьютерной системе пользователя программы. Возможность получения несанкционированного доступа может также образоваться в результате наличия ошибок в программах или операционных системах.

Техника Phishing.

Техника с названием phishing используется с целью выманить у пользователя Интернета персональную информацию (пароли, пин-коды и т.д.). При этом злоумышленники могут направлять ему поддельные сообщения электронной почты. В этих сообщениях, отправленных, например, от имени популярного Web-сайта или банка, может говориться о том, что по той или иной причине пользователь должен выслать банку пароль или пин-код.

Для ввода пароля пользователь заманивается на поддельный сайт, повторяющий по своему дизайну сайт банка, другой компании или организации. Пользователю могут демонстрироваться всплывающие окна, копирующие сайт.

Программы Spyware.

Вредоносные программы Spyware устанавливаются на компьютер пользователя и собирают различную информацию о действиях пользователя. Обычно это информация, ценная для маркетологов, которая после сбора отсылается разработчику программы через Интернет.

Программы Adware.

Программы adware отображают рекламную информацию на компьютере. Эти программы могут отображать на экране всплывающие окна с рекламными баннерами и текстом, даже при отсутствии подключения к Интернету.

Клавиатурные шпионы.

Одна из наиболее распространенных разновидностей программных закладок — клавиатурные шпионы (кейлоггеры). Такие программные закладки нацелены на перехват паролей пользователей операционной системы, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам.

Поведение клавиатурных шпионов в общем случае является довольно традиционным: типовой клавиатурный шпион обманным путем завладевает пользовательскими паролями, а затем переписывает эти пароли туда, откуда их может без особого труда извлечь злоумышленник. Различия между

клавиатурными шпионами касаются только способа, который применяется ими для перехвата пользовательских паролей. Соответственно все клавиатурные шпионы делятся на три типа — имитаторы, фильтры и заместители.

Парольные взломщики.

Эффективным методом взлома парольной защиты операционной системы является метод, при котором атаке подвергается системный файл, содержащий информацию о ее легальных пользователях и их паролях. Однако любая современная операционная система надежно защищает при помощи шифрования пользовательские пароли, которые хранятся в этом файле. Доступ к таким файлам, как правило, по умолчанию запрещен даже для системных администраторов. Тем не менее, в ряде случаев злоумышленнику удается путем различных ухищрений получить в свое распоряжение файл с именами пользователей и их зашифрованными паролями. В этом случае используются так называемые парольные взломщики — специализированные программы, которые служат для взлома паролей операционных систем.

Криптографические алгоритмы, применяемые для шифрования паролей пользователей в современных операционных системах, в подавляющем большинстве случаев являются слишком стойкими, чтобы можно было надеяться отыскать методы их дешифрования, которые окажутся более эффективными, чем тривиальный перебор возможных вариантов. Поэтому парольные взломщики иногда просто шифруют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой операционной системе, и сравнивают результаты шифрования с тем, что записано в системном файле, где находятся шифрованные пароли ее пользователей. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов. Данный способ позволяет взломать все пароли, если известно их представление в зашифрованном виде и они содержат только символы из данного набора.

Для более эффективного подбора паролей парольные взломщики обычно используют так называемые словари, представляющие собой заранее сформированный список слов, наиболее часто применяемых на практике в качестве паролей.

Лекция №7. Защита от вредоносного ПО

Цель лекций: ознакомить студентов с принципами работы и функциональностью антивирусного программного обеспечения, видами сканеров безопасности.

Антивирусное программное обеспечение.

Невозможность существования абсолютного антивируса была доказана Фредом Коэном математически на основе теории конечных автоматов.

В антивирусном ПО используются следующие термины:

«Ложное срабатывание» (False positive) — детектирование вируса в незараженном объекте. Обратный термин — «False negative», т.е. недетектирование вируса в зараженном объекте.

«Сканирование по запросу» («on-demand») — поиск вирусов по запросу пользователя.

«Сканирование на-лету» («real-time», «on-the-fly») — постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Качество антивирусной программы можно определить по следующим позициям:

- надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;
- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (Word, Excel), упакованных и архивированных файлов;
- отсутствие «ложных срабатываний»;
- многоплатформенность антивирусного программного обеспечения;
- возможность лечения зараженных объектов;
- периодичность обновления;
- существование серверных версий с возможностью проверки сетевых дисков;
- скорость работы и другие полезные функции;

Антивирусное ПО может использовать следующие методы обнаружения вирусов и других вредоносных программ:

- сканирование;
- эвристический анализ (блокирование подозрительных действий);
- CRC-сканирование (обнаружение изменений);
- анализ сетевого трафика;
- анализ баз данных почтовых программ;
- обнаружение вирусов в системе автоматизации документооборота.

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы «эвристического сканирования», т.е. анализ последовательности команд в проверяемом

объекте, набор некоторой статистики и принятие решения («возможно заражен» или «не заражен») для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Эвристический анализ не дает полной гарантии обнаружения любых новых вирусов. Кроме того, эвристический анализатор может принять «безобидную» программу за вредоносную. Это происходит в тех случаях, когда программа выполняет какие-либо действия, характерные для вирусов или вредоносных программ другого типа. Эвристический анализ отнимает немало процессорного времени. Поэтому, настраивая антивирусную программу, пользователь может отключить эвристический анализатор. Учитывая, что без эвристического анализатора антивирусная программа не сможет обнаружить полиморфные и шифрующиеся, а также новые вирусы, такое отключение приведет к снижению надежности антивирусной защиты.

Наиболее эффективной методикой обнаружения и нейтрализации вредоносных программ, распространяющихся по каналам электронной почты, является анализ трафика электронной почты непосредственно на почтовом сервере. При этом антивирусные программы проверяют данные, проходящие через почтовый сервер, и удаляют из них вредоносные объекты еще до того, как они попадут на компьютер пользователя. Антивирусы, работающие на почтовом сервере, сканируют трафик электронной почты, исключая распространение вредоносных программ вместе с почтовыми сообщениями. Для передачи сообщений электронной почты используются протоколы SMTP, POP3 и IMAP. Специализированные антивирусы, работающие на почтовых серверах, способны анализировать потоки данных, передаваемые с использованием этих протоколов, предотвращая распространение вредоносных программных объектов через электронную почту.

Сканеры также можно разделить на две категории — «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на-лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам — размеры антивирусных баз, которые сканерам приходится «таскать за собой», и относительно небольшую скорость поиска вирусов.

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения. К недостаткам относятся существование путей обхода защиты блокировщиков, большое количество срабатываний, требующих от пользователя принятия решения.

Лекция №8. Проблемы безопасности протоколов TCP/IP

Цель лекций: рассмотреть наиболее распространенные методы и инструменты злоумышленников при осуществлении атаки на сеть.

Прежде чем перейти к разбору конкретных приемов, классифицируем действия злоумышленника — атаки, направленные против какого-либо узла (или, возможно, целой сети). Злоумышленник ставит перед собой определенную цель:

- перехват (и, возможно, модификация) данных, передаваемых через сеть от одного узла другому;
- имперсонация (обезличивание, spoofing) (узел злоумышленника выдает себя за другой узел, чтобы воспользоваться какими-либо привилегиями имитируемого узла);
- несанкционированное подключение к сети;

- несанкционированная передача данных (обход правил фильтрации IP-трафика в сетях, защищенных брандмауэрами);
- принуждение узла к передаче данных на завышенной скорости;
- приведение узла в состояние, когда он не может нормально функционировать, передавать и принимать данные.

1. Методы и инструменты

Для достижения своих целей злоумышленник использует:
- прослушивание сети (sniffing);
- сканирование сети;
- генерация пакетов.

Прослушивание сети.

Прослушивание сети Ethernet является тривиальной задачей: для этого необходимо перевести сетевой интерфейс в режим прослушивания. Легко доступны программы, не только записывающие весь трафик в сегменте Ethernet, но и выполняющие его отбор по установленным критериям.

Среди других сетевых технологий подвержены прослушиванию сети FDDI и радиосети (например Radio Ethernet). Несколько сложнее для злоумышленника извлечь трафик из телефонных выделенных и коммутируемых линий — главным образом, из-за сложности физического доступа и подключения к таким линиям. Однако следует помнить, что злоумышленник может оккупировать промежуточный маршрутизатор и таким образом получить доступ ко всему транзитному трафику, независимо от используемых технологий на уровне доступа к сети.

Ограничить область прослушивания в сети Ethernet можно разбиением сети на сегменты с помощью коммутаторов. В этом случае злоумышленник, не прибегая к активным действиям, может перехватить только кадры, получаемые или отправляемые узлами сегмента, к которому он подключен. Единственным способом борьбы с прослушиванием сегмента Ethernet является шифрование данных.

Сканирование сети.

Сканирование сети имеет своей целью выявление подключенных к сети компьютеров и определение работающих на них сетевых сервисов (открытых портов TCP или UDP). Первая задача выполняется посылкой ICMP-сообщений Echo с помощью программы ping с последовательным перебором адресов узлов в сети. Если отправить Echo-сообщение по широковещательному адресу, то на него ответят все компьютеры, поддерживающие обработку таких сообщений.

Администратор сети может обнаружить попытки сканирования путем анализа трафика в сети и отслеживания Echo-сообщений, за короткий промежуток времени посылаемых последовательно по всем адресам сети.

Программа traceroute поможет в определении топологии сети и обнаружении маршрутизаторов.

Генерация пакетов.

Под генерацией пакетов понимается создание и отправка специально сконструированных датаграмм или кадров, позволяющих злоумышленнику выполнить ту или иную атаку. Особо выделим здесь фальсификацию пакетов,

то есть создание IP-датаграмм или кадров уровня доступа к сети, направленных якобы от другого узла (spoofing).

Генерация датаграмм или кадров произвольного формата и содержания производится не менее просто, чем прослушивание сети Ethernet. На многочисленных сайтах Интернета злоумышленник может найти уже готовые программы, генерирующие пакеты целенаправленно для выполнения какой-либо атаки или сканирования сети. Применение таких программ часто не требует от злоумышленника ни квалификации программиста, ни понимания принципов работы сети, что делает многие из описанных атак, особенно атаки типа «отказ в обслуживании», широко доступными для исполнения.

Перехват данных.

Простейшей формой перехвата данных является прослушивание сети. В этом случае злоумышленник может получить массу полезной информации: имена пользователей и пароли (многие приложения передают их в открытом виде), адреса компьютеров в сети, в том числе адреса серверов и запущенные на них приложения, адрес маршрутизатора, собственно передаваемые данные, которые могут быть конфиденциальными (например, тексты электронных писем) и т. п.

Ложные ARP-ответы.

Для перехвата трафика между узлами A и B, расположенными в одной IP-сети, злоумышленник использует протокол ARP. Он рассылает сфальсифицированные ARP-сообщения так, что каждый из атакуемых узлов считает MAC-адрес злоумышленника адресом своего собеседника (рисунок 1).

Для обнаружения ARP-атак администратор должен вести базу данных соответствия MAC- и IP-адресов всех узлов сети и использовать программу arpwatch, которая прослушивает сеть и уведомляет администратора о замеченных нарушениях. Если сеть разделена на сегменты коммутаторами, то администратор должен настроить их таким образом, чтобы в сегмент, где находится станция администратора, перенаправлялись кадры из всех сегментов сети вне зависимости от того, кому они предназначены.

Использование статических ARP-таблиц, по крайней мере — на ключевых узлах (серверах, маршрутизаторах), защитит их от ARP-атаки, правда, за счет накладных расходов на поддержку этих таблиц в актуальном состоянии.

Пользователю на атакуемом хосте, не снабженном статической ARP-таблицей, крайне сложно заметить, что он подвергся ARP-атаке, поскольку представляется маловероятным, что пользователь помнит MAC-адреса других узлов своей сети и периодически проверяет ARP-таблицу своего компьютера.

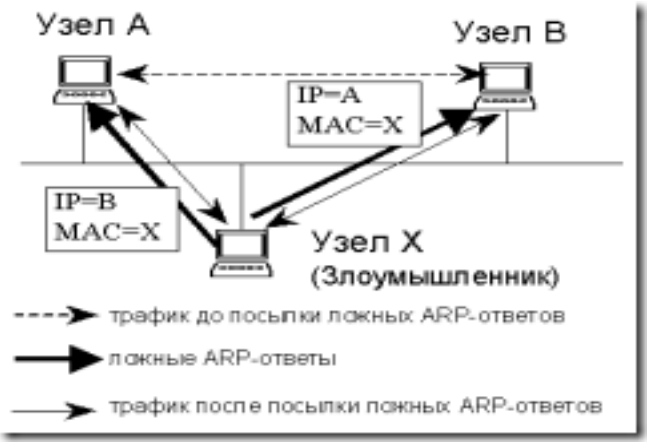

Рисунок 6.1 - Схема ARP-атаки

Навязывание ложного маршрутизатора.

Для перехвата трафика, направленного от некоторого узла A в другую сеть, злоумышленник может навязать хосту свой адрес в качестве адреса маршрутизатора, которому должны быть переданы отправляемые узлом A данные. В этом случае узел A будет направлять трафик на узел злоумышленника, который после анализа и, возможно, модификации данных, отправит их далее настоящему маршрутизатору.

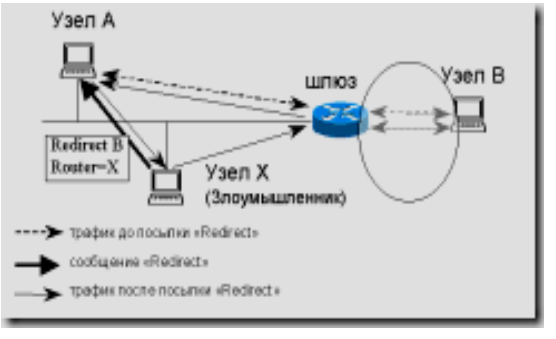

Рисунок 6.2 - Навязывание ложного маршрутизатора с помощью ICMP Redirect

На атакуемом узле сообщение Redirect отобразится в виде появившейся строки в таблице маршрутов, направляющей данные для хоста B через узел X. Кроме того, программа traceroute скорее всего покажет дополнительный промежуточный узел на пути к B.

Атака при конфигурировании хоста.

В некоторых случаях навязывание ложного маршрутизатора может быть произведено с помощью ICMP-сообщения Router Advertisement или через протокол DHCP.

Атака на протоколы маршрутизации.

Если злоумышленник хочет перехватить трафик между узлами сети P и узлами сети Q, и при этом не находится ни в одной из сетей P или Q, но расположен на пути между ними, он может попытаться ввести в заблуждение маршрутизаторы. Маршрутизаторы не реагируют на сообщения ICMP Redirect, поэтому для успешной атаки необходимо, чтобы они использовали какой-либо протокол маршрутизации. В этом случае злоумышленник может

сформировать подложные сообщения протокола маршрутизации с целью переключения требуемых маршрутов на себя. Например (рисунок 3) узел X, приняв широковещательные RIP-сообщения, рассылаемые узлами A (вектор P=3) и B (вектор Q=2), отправляет сообщение с вектором Q=1 на индивидуальный адрес маршрутизатора A, а сообщение P=2 — на индивидуальный адрес B. Аутентификация TCP-сегментов с помощью алгоритма MD5 поможет изсключить данную атаку.

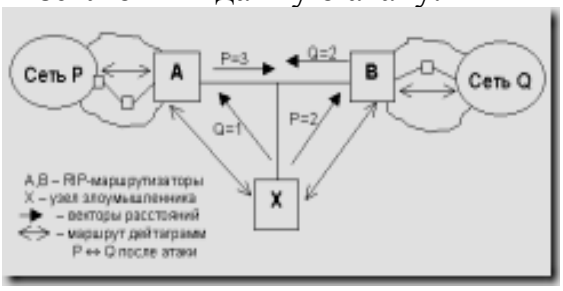

Рисунок 6.3 - Навязывание ложного RIP-маршрутизатора X для перехвата трафика между сетями P и Q

Лекция №9. Выявление уязвимостей компьютерных сетей

Цель лекций: научить студентов выявлять уязвимости компьютерных сетей. Рассмотреть общие меры по повышению безопасности сети.

Выявление уязвимостей компьютерных сетей.

Системы обнаружения атак.

Существует три этапа осуществления атаки. Первый, подготовительный, этап заключается в поиске предпосылок для осуществления той или иной атаки. На этом этапе ищутся уязвимости, использование которых приводит к реализации атаки, т.е. ко второму этапу. На третьем этапе завершается атака, «заметаются» следы и т.д. При этом первый и третий этапы сами по себе могут являться атаками.

Существующие механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа и т.д. работают только на втором этапе, т.е., по существу, они являются средствами блокирующими, а не упреждающими атаки. В абсолютном большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. И даже если они смогли предотвратить ту или иную атаку, то намного более эффективным было бы упреждение атак, т.е. устранение самих предпосылок реализации вторжений. Комплексная система обеспечения информационной безопасности должна работать на всех трех этапах осуществления атаки. И обеспечение адекватной защиты на третьем, завершающем, этапе не менее важно, чем на первых двух. Ведь только в этом случае можно реально оценить ущерб от «успешной» атаки, а также разработать меры по устранению дальнейших попыток реализовать аналогичную атаку.

Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Первый, и самый распространенный, способ - это обнаружение уже

реализуемых атак. Этот способ применяется в «классических» системах обнаружения атак (например, RealSecure компании Internet Security Systems), межсетевых экранах и т.п. Однако, «недостаток» средств данного класса в том, что атаки могут быть реализованы повторно. Второй путь - предотвратить атаки еще до их реализации. Осуществляется это путем поиска уязвимостей, которые могут быть использованы для реализации атаки. И, наконец, третий путь - обнаружение уже совершенных атак и предотвращение их повторного осуществления.

Системы, функционирующие на первом этапе осуществления атак и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки. Иначе средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners). Обычно системы анализа защищенности не принято относить к классу средств обнаружения атак, однако, если следовать описанным выше этапам осуществления атаки, то такое отнесение вполне логично.

Системы, функционирующие на втором этапе осуществления атаки и позволяющие обнаружить атаки в процессе их реализации, т.е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Помимо этого, можно выделить такой класс средств обнаружения атак, как обманные системы.

Системы, функционирующие на третьем этапе осуществления атаки и позволяющие обнаружить уже совершенные атаки. Эти системы делятся на два класса - системы контроля целостности, обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации.

Системы контроля целостности.

Системы контроля целостности работают по замкнутому циклу, обрабатывая файлы, системные объекты и атрибуты системных объектов с целью получения контрольных сумм; затем они сравнивают их с предыдущими контрольными суммами, отыскивая изменения. Когда изменение обнаружено, система посылает сообщение администратору, фиксируя время, соответствующее вероятному времени изменения. Если вновь вернуться к этапам реализации атаки, то системы этого класса функционируют на третьем этапе, т.е. они могут однозначно сказать, происходила атака (точнее изменение контролируемого объекта) или нет.

Обманные системы.

Обычно, когда речь заходит об обмане в области информационной безопасности, то здесь используются методы, которые применяют злоумышленники, т.е. лазейки для обхода используемых средств защиты, будь то кража паролей и работа от имени авторизованного пользователя или несанкционированное использование модемов. Обман может сослужить хорошую службу не только для злоумышленников, но и для защиты корпоративных ресурсов. Существует множество различных вариантов использования обмана в благих целях:

- сокрытие;

- камуфляж;
- дезинформация.

Однако не стоит думать, что при помощи средств анализа защищенности можно тестировать только возможность несанкционированного доступа в корпоративную сеть из сетей открытого доступа (например, Internet). Эти средства с не меньшим успехом могут быть использованы для анализа некоторых сегментов или узлов внутренней сети организации. Системы анализа защищенности могут быть использованы:

- для оценки уровня безопасности организации;
- для контроля эффективности настройки сетевого, системного и прикладного программно-аппаратного обеспечения;
- внешними аудиторскими и консалтинговыми компаниями, осуществляющими информационные обследования сетей заказчиков;
- для тестирования и сертификации того или иного программно-аппаратного обеспечения.

Таблица 7.1 - Средства анализа защищенности.

Название	Производитель	Категория
Internet Scanner	Internet Security Systems	На уровне сети
System Scanner	Internet Security Systems	На уровне ОС
Database Scanner	Internet Security Systems	На уровне СУБД
Cisco Secure Scanner	Cisco Systems	На уровне сети
CyberCop Scanner	Network Associates	На уровне сети
WebTrends Security Analyzer	WebTrends Corporation	На уровне сети
Enterprise	Security Manager	Symantec
SFProtect	Hewlett Packard	На уровне сети, ОС, СУБД
Nessus	Свободно распространяется	На уровне сети

Поскольку постоянно появляются новые уязвимости, то для их эффективного обнаружения необходимо постоянно обновлять базу данных системы анализа защищенности. В идеале разрыв между появлением информации об уязвимости в различных «хакерских» источниках и появлением сигнатуры в базе данных системы обнаружения должен отсутствовать. Но как бы часто не обновлялась база данных уязвимостей, существует временной промежуток между сообщением о новой уязвимости и появлением проверки для нее.

Существует два основных механизма, при помощи которых сканер проверяет наличие уязвимости - сканирование (scan) и зондирование (probe).

Сканирование - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам.

Зондирование - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость.

Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость.

Общие меры по повышению безопасности сети.

1. *Оперативная установка исправлений для программ (Patching).* Системные администраторы должны защищать самые важные свои системы, оперативно устанавливая исправления для программ на них. Тем не менее, установить исправления для программ на всех хостах в сети трудно, так как исправления могут появляться достаточно часто. В этом случае надо обязательно вносить исправления в программы на самых важных хостах.

2. *Обнаружение вирусов и троянских коней.* Для максимальной эффективности они должны быть установлены на всех компьютерах в сети. На установку антивирусных программ на всех компьютерах и регулярное обновление антивирусных баз в них может уходить достаточно много времени - но иначе это средство не будет эффективным. Пользователей следует учить, как им самим делать эти обновления, но при этом нельзя полностью полагаться на них. Помимо обычной антивирусной программы на каждом компьютере, мы необходимо сканирование приложений к электронным письмам на почтовом сервере. Таким образом, можно обнаружить большинство вирусов до того, как они достигнут машин пользователей.

3. *Межсетевые экраны.* Межсетевые экраны - самое важное средство защиты сети организации. Они контролируют сетевой трафик, входящий в сеть и выходящий из нее. Межсетевой экран может блокировать передачу в сеть какого-либо вида трафика или выполнять те или иные проверки другого вида трафика. Хорошо сконфигуированный межсетевой экран в состоянии остановить большинство известных компьютерных атак.

4. *Вскрыватели паролей (Password Crackers).* Хакеры часто используют малоизвестные уязвимые места в компьютерах для того, чтобы украсть файлы с зашифрованными паролями. Затем они используют специальные программы для вскрытия паролей, которые могут обнаружить слабые пароли в этих зашифрованных файлах. Хотя это средство используются злоумышленниками, оно будет также полезно и системным администраторам, чтобы своевременно обнаружить слабые пароли.

5. *Шифрование.* Атакующие часто проникают в сети с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей. Поэтому соединения с удаленными машинами, защищаемые с помощью пароля, должны быть зашифрованы. Это особенно важно в тех случаях, если соединение осуществляется по Интернет или с важным сервером. Имеется ряд коммерческих и бесплатных программ для шифрования трафика TCP/IP (наиболее известен SSH).

6. *Сканеры уязвимых мест.* Это программы, которые сканируют сеть в поисках компьютеров, уязвимых к определенным видам атак. Сканеры имеют большую базу данных уязвимых мест, которую они используют при проверке того или иного компьютера на наличие у него уязвимых мест.

7. *Грамотное конфигурирование компьютеров в отношении безопасности.*

8. *Средства для поиска подключенных модемов.* Для поиска подключенных модемов атакующие могут использовать программы обзвонки большого числа телефонных номеров. Так как пользователи обычно конфигурируют свои компьютеры сами, они часто оказываются плохо защищенными и дают атакующему еще одну возможность для организации атаки на сеть. Системные администраторы должны регулярно использовать программы для проверки телефонных номеров своих пользователей и обнаружения сконфигурированных подобным образом компьютеров.

9. *Рекомендации по безопасности (security advisories).* Рекомендации по безопасности - это предупреждения, публикуемые группами по борьбе с компьютерными преступлениями и производителями программ о недавно обнаруженных уязвимых местах. Рекомендации обычно описывают самые серьезные угрозы, возникающие из-за этих уязвимых мест и поэтому являются занимающими мало времени на чтение, но очень полезными. Они описывают угрозу и дают довольно конкретные советы о том, что нужно сделать для устранения данного уязвимого места. Двумя самыми полезными являются рекомендации, которые публикует группа по борьбе с компьютерными преступлениями CIAC и CERT

10. *Средства обнаружения атак (Intrusion Detection).* Системы обнаружения атак оперативно обнаруживают компьютерные атаки. Они могут быть установлены за межсетевым экраном, чтобы обнаруживать атаки, организуемые изнутри сети. Или они могут быть установлены перед межсетевым экраном, чтобы обнаруживать атаки на межсетевой экран. Средства этого типа могут иметь разнообразные возможности.

11. *Средства выявления топологии сети и сканеры портов.* Эти программы позволяют составить полную картину того, как устроена ваша сеть и какие компьютеры в ней работают, а также выявить все сервисы, которые работают на каждой машине. Атакующие используют эти средства для выявления уязвимых компьютеров и программ на них. Системные администраторы должны использовать эти средства для наблюдения за тем, какие программы и на каких компьютерах работают в их сети. С их помощью можно обнаружить неправильно сконфигурированные программы на компьютерах и установить исправления на них.

12. *Инструкции по действию в критических ситуациях.* В каждой сети, независимо от того, насколько она безопасна, происходят какие-либо события, связанные с безопасностью (может быть даже ложные тревоги). Сотрудники организации должны заранее знать, что нужно делать в том или ином случае.

13. *Политики безопасности.* Организации должны написать политику безопасности, в которой определялся бы ожидаемый уровень защиты, который должен быть везде единообразно реализован. Самым важным аспектом политики является выработка единых требований к тому, какой трафик должен пропускаться через межсетевые экраны сети. Также политика должна определять как и какие средства защиты (например, средства обнаружения атак или сканеры уязвимых мест) должны использоваться в сети. Для достижения единого уровня безопасности политика должна

определять стандартные безопасные конфигурации для различных типов компьютеров.

14. *Тестирование межсетевых экранов и WWW-серверов на устойчивость к попыткам их блокирования.* Атаки на блокирование компьютера распространены в Интернет. Атакующие постоянно выводят из строя WWW-сайты, перегружают компьютеры или переполняют сети бессмысленными пакетами. Сети, заботящиеся о безопасности, могут организовать атаки против себя сами, чтобы определить, какой ущерб может быть нанесен им.

Лекция №10. Экранирование и межсетевые экраны

Цель лекций: углубить и закрепить знания студентов в области сетевой безопасности. Ознакомить с принципами экранирования и функциями межсетевого экрана.

Экранирование и межсетевые экраны.

Основные понятия.

Межсетевой экран (МЭ) представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Мы будем использовать понятия межсетевой экран (МЭ), брандмауэр, firewall, шлюз с установленным дополнительным программным обеспечением firewall, как эквивалентные.

Формальная постановка задачи экранирования, состоит в следующем. Пусть имеется два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рисунок 8.1). Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

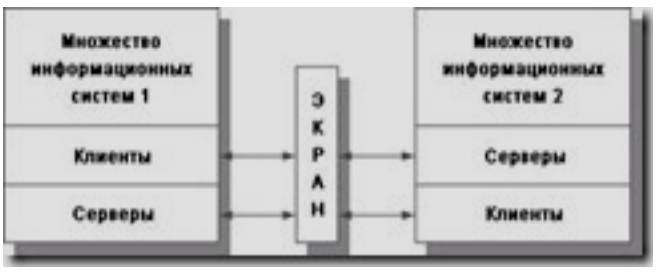

Рисунок 8.1 - Экран как средство разграничения доступа

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров,

проанализировав данные, может задержать (не пропустить) их, а может и сразу «перебросить» за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рисунок 8.2).

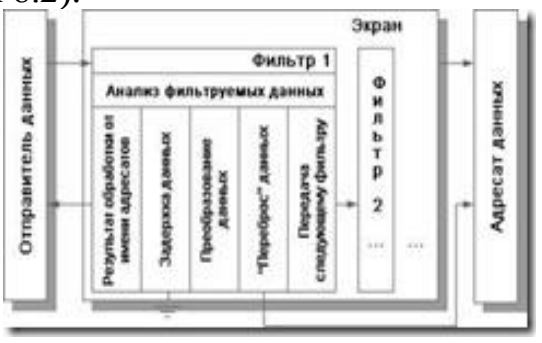

Рисунок 8.2 - Экран как последовательность фильтров

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором – о внутреннем. Межсетевой экран – идеальное место для встраивания средств активного аудита. МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

Принципы работы межсетевых экранов.

Существует два основных способа создания наборов правил межсетевого экрана: «включающий'» и «исключающий». Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.

Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием «межсетевого экрана с сохранением состояния». Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением

состояния и без сохранения состояния, что оптимально для реальных применений.

Лекция №11. Несанкционированное подключение к сети

Цель лекций: ознакомить студентов с методами несанкционированного подключения к сети и вариантами защиты.

Для незаконного подключения к сети злоумышленник должен иметь физическую возможность такого подключения. В крупных корпоративных и особенно университетских сетях такая возможность часто имеется. Следующим шагом для злоумышленника является конфигурирование параметров стека TCP/IP его компьютера.

Прослушивая сеть (сегмент сети) злоумышленник может определить, какие IP-адреса имеют узлы сети, с помощью ICMP Echo-запросов (программа ping) определить, какие адреса не используются (или компьютеры выключены), найти IP-адрес маршрутизатора по умолчанию. После этого злоумышленник может присвоить себе неиспользуемый адрес.

Если в сети имеется сервер DHCP, который предоставляет IP-адреса всем желающим, то он полностью сконфигурирует узел злоумышленника без всяких усилий со стороны последнего. Это событие будет зарегистрировано в журнале сервера.

Для предотвращения несанкционированного подключения к сети администратор должен использовать статическую ARP-таблицу на маршрутизаторе (и ключевых хостах-серверах) и программу arpwatch. Статическая ARP-таблица не позволит злоумышленнику получить ни одну датаграмму от узла, который ее использует, поскольку MAC-адрес злоумышленника, естественно, не значится в таблице. Программа arpwatch уведомит администратора о появлении узла с неизвестным MAC-адресом.

Однако, если злоумышленник, определив IP- и MAC-адреса какого-либо компьютера в своей сети, дождется его выключения (или проведет против него атаку «отказ в обслуживании», приводящую к неспособности атакуемого хоста работать в сети), а потом присвоит себе его MAC- и IP-адреса, то обнаружить такого злоумышленника будет невозможно и все его действия будут приписаны атакованному хосту.

Несанкционированный обмен данными.

С целью обеспечения безопасности внутренней (корпоративной) сети на шлюзе могут использоваться фильтры, препятствующие прохождению определенных типов датаграмм. Датаграммы могут фильтроваться по IP-адресам отправителя или получателя, по протоколу (поле Protocol IP-датаграммы), по номеру порта TCP или UDP, по другим параметрам, а также по комбинации этих параметров. Злоумышленник может использовать следующие два приема для проникновения через некоторые фильтры.

Лекция №12. Безопасность электронной коммерции

Цель лекций: ознакомить студентов с классификацией возможных типов мошенничества в электронной коммерции и основными протоколами обеспечивающими безопасность в данной области.

Широкое внедрение интернета не могло не отразиться на развитии электронного бизнеса.

Одним из видов электронного бизнеса считается электронная коммерция. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка и расчеты) осуществляются с помощью Интернета. Поэтому в такой интерпретации обычно полагают, что покупка относится к электронной коммерции, если, как минимум, маркетинг (организация спроса) и расчеты производятся средствами Интернета. Более узкая трактовка понятия «электронная коммерция» характеризует системы безналичных расчетов на основе пластиковых карт.

Ключевым вопросом для внедрения электронной коммерции является безопасность.

Высокий уровень мошенничества в интернете является сдерживающим фактором развития электронной коммерции. Покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери. Люди главным образом используют интернет в качестве информационного канала для получения интересующей их информации. Лишь немногим более 2% всех поисков по каталогам и БД в интернете заканчиваются покупками.

Приведем классификацию возможных типов мошенничества в электронной коммерции:

- транзакции (операции безналичных расчетов), выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т.п.);
- получение данных о клиенте через взлом БД торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные;
- магазины-бабочки, возникающие, как правило, на непродолжительное время, для того, чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;
- увеличение стоимости товара по отношению к предлагавшейся покупателю цене или повтор списаний со счета клиента;
- магазины или торговые агенты, презназначенные для сбора информации о реквизитах карт и других персональных данных покупателя.

Протокол SSL.

Протокол SSL (Secure Socket Layer) был разработан американской компанией Netscape Communications. SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, NNTP, FTP и т.д.) и транспортными протоколами (TCP/IP) с помощью современной криптографии

в соединениях «точка-точка». Ранее можно было без особых технических ухищрений просматривать данные, которыми обмениваются между собой клиенты и серверы. Был даже придуман специальный термин для этого – «sniffer».

Протокол SSL предназначен для решения традиционных задач обеспечения защиты информационного взаимодействия:

- пользователь и сервер должны быть взаимно уверены, что они обмениваются информацией не с подставными абонентами, а именно с теми, которые нужны, не ограничиваясь паролевой защитой;
- после установления соединения между сервером и клиентом весь информационный поток между ними должен быть защищен от несанкционированного доступа;
- при обмене информацией стороны должны быть уверены в отсутствии случайных или умышленных искажений при ее передаче.

SSL на сегодня является наиболее распространенным протоколом, используемым при построении систем электронной коммерции. С его помощью осуществляется 99% всех транзакций. Широкое распространение SSL объясняется в первую очередь тем, что он является составной частью всех браузеров и Web-серверов. Другое достоинство SSL - простота протокола и высокая скорость реализации транзакции.

В то же время, SSL обладает рядом существенных недостатков:

- покупатель не аутентифицируется;
- продавец аутентифицируется только по URL;
- цифровая подпись используется только при аутентификации в начале установления SSL-сессии. Для доказательства проведения транзакции при возникновении конфликтных ситуаций требуется либо хранить весь диалог покупателя и продавца, что дорого с точки зрения ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение товара покупателем;
- не обеспечивается конфиденциальность данных о реквизитах карты для продавца.

Протокол SET.

Другой протокол безопасных транзакций в Интернете - **SET** (Security Electronics Transaction). SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и VISA при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя самый защищенный на настоящее время механизм выполнения платежей. SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернет. SET обеспечивает кросс-аутентификацию счета держателя карточки, продавца и банка продавца для проверки готовности оплаты товара, целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET можно назвать стандартной технологией или системой протоколов

выполнения безопасных платежей с использованием пластиковых карточек через Интернет.

SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки, происходящей в Интернет, с помощью криптографии, применяя, в том числе, и цифровые сертификаты.

Объем потенциальных продаж в области электронной коммерции ограничивается достижением необходимого уровня безопасности информации, который обеспечивают вместе покупатели, продавцы и финансовые институты, обеспокоенные вопросами обеспечения безопасности платежей через Интернет. Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличии от других протоколов, позволяет решать указанные задачи защиты информации.

Лекция №13. Безопасность электронных платежных систем

Цель лекций: идентифицировать, что называется электронной платежной системой и рассмотреть принципы безопасной работы с электронными платежными системами.

Современную практику банковских операций, торговых сделок и взаимных платежей невозможно представить без расчетов с применением пластиковых карт.

Система безналичных расчетов с помощью пластиковых карт называется *электронной платежной системой.*

Для обеспечения нормальной работы электронная платежная система должна быть надежно защищена.

С точки зрения информационной безопасности в системах электронных платежей существуют следующие уязвимые места:

- пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом;
- обработка информации внутри огранизаций отправителя и получателя сообщений;
- доступ клиентов к средствам, аккумилированным на счетах.

Пересылка платежных и других сообщений связана с такими особенностями:

- внутренние системы организаций отправителя и получателя должны обеспечивать необходимую защиту при обработке электронных документов (защита оконечных систем);
- взаимодействие отправителя и получателя электронного документа осуществляется опосредованно - через канал связи.

Эти особенности порождают следующие проблемы:

- взаимное опознание абонентов (проблема установления взаимной подлинности при установлении соединения);
- защита электронных документов, передаваемых по каналам связи (проблема обеспечения конфиденциальности и целостности документов);

- защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

- обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости).

Для обеспечения функций защиты информации на отдельных узлах системы электронных платежей должны быть реализованы следующие механизмы защиты:

- управление доступом на оконечных системах;
- контроль целостности сообщения;
- обеспечение конфиденциальности сообщения;
- взаимная аутентификация абонентов;
- невозможность отказа от авторства сообщения;
- гарантии доставки сообщения;
- невозможность отказа от принятия мер по сообщения;
- регистрация последовательности сообщений;
- контроль целостности последовательности сообщений.

Итак, в качестве платежного средства в электронной платежной системе используются электронные пластиковые карты.

Электронная пластиковая карта - это носитель информации, который идентифицирует владельца и хранит определенные учетные данные.

Различают кредитные и дебетовые карты.

Кредитные карты являются наиболее распространенным видом пластиковых карт. К ним относятся карты общенациональных систем США Visa и MasterCard, American Express и ряда других. Эти карты предъявляют для оплаты товаров и услуг. При оплате с помощью кредитной карты банк покупателя открывает ему кредит на сумму покупки, а затем через некоторое время (обычно 25 дней) присылает счет по почте. Покупатель должен вернуть оплаченный чек (счет) обратно в банк. Естественно, подобную схему банк может предложить только наиболее состоятельным и проверенным из своих клиентов, которые имеют хорошую кредитную историю перед банком или солидные вложения в банк в виде депозитов, ценностей или недвижимости.

Владелец *дебетовой карты* должен заранее внести на свой счет в банке-эмитенте определенную сумму. Размер этой суммы определяет лимит доступных средств. При осуществлении расчетов с использованием этой карты соответственно уменьшается и лимит. Для возобновления или увеличения лимита владелец должен вновь внести деньги на свой счет. Для страхования временного разрыва между моментом осуществления платежа и моментом получения банком соответствующей информации на счете клиента должен поддерживаться неснижаемый остаток.

Лекция №14. Безопасность Wi-Fi сетей

Цель лекций: ознакомить студентов с правилами безопасности при работе с беспроводными сетями.

Устройства стандарта 802.11 связываются друг с другом, используя в качестве переносчика данных сигналы, передаваемые в диапазоне радиочастот. Данные передаются по радио отправителем, полагающим, что приемник также работает в выбранном радиодиапазоне. Недостатком такого механизма является то, что любая другая станция, использующая этот диапазон, тоже способна принять эти данные.

Если не использовать какой-либо механизм защиты, любая станция стандарта 802.11 сможет обработать данные, посланные по беспроводной локальной сети, если только ее приемник работает в том же радиодиапазоне. Для обеспечения хотя бы минимального уровня безопасности необходимы следующие компоненты:

- средства для принятия решения относительно того, кто или что может использовать беспроводную LAN. Это требование удовлетворяется за счет механизма аутентификации, обеспечивающего контроль доступа к LAN;
- средства защиты информации, передаваемой через беспроводную среду. Это требование удовлетворяется за счет использования алгоритмов шифрования.

В спецификации стандарта 802.11 регламентировано применение механизма аутентификации устройств с открытым и с совместно используемым ключом и механизма WEP, обеспечивающего защищенность данных на уровне проводных сетей. Оба алгоритма аутентификации, с открытым и с совместно используемым ключом, основаны на WEP-шифровании и применении WEP-ключей для контроля доступа.

WEP

Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP. Этот алгоритм основан на применении симметричного поточного шифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 бит статично конфигурируются на клиентских устройствах и в точках доступа. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений.

Механизмы аутентификации стандарта 802.11

Спецификация стандарта 802.11 оговаривает два механизма, которые могут применяться для аутентификации клиентов WLAN:

- открытая аутентификация (open authentication);
- аутентификация с совместно используемым ключом (shared key authentication).

Открытая аутентификация, по сути, представляет собой алгоритм с нулевой аутентификацией (null authentication algorithm). Точка доступа принимает любой запрос на аутентификацию. Это может быть просто бессмысленный сигнал, используемый для указания на применение именно этого алгоритма аутентификации, тем не менее открытая аутентификация играет определенную роль в сетях стандарта 802.11. Столь простые требования к аутентификации позволяют устройствам быстро получить доступ к сети.

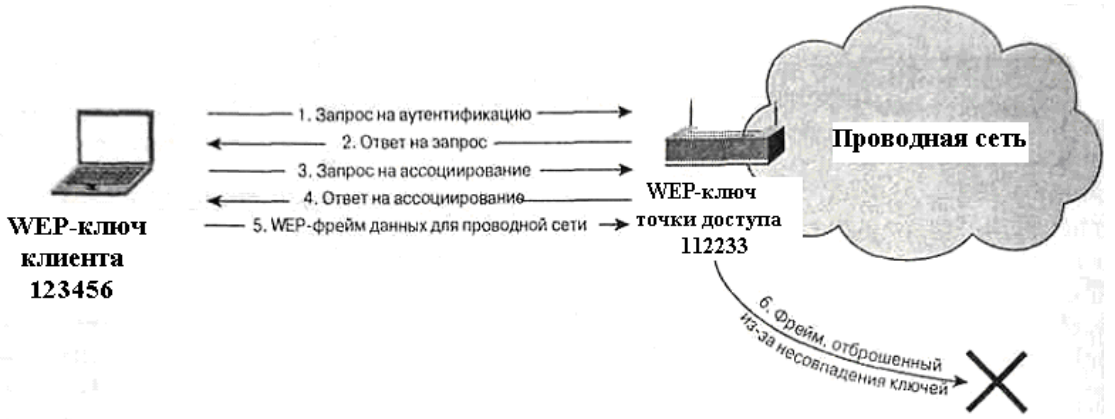

Рисунок 12.1 - Процесс открытой аутентификации при различии WEP-ключей

В отличие от открытой аутентификации, при аутентификации с совместно используемым ключом требуется, чтобы клиентская станция и точка доступа были способны поддерживать WEP и имели одинаковые WEP-ключи.

Для получения достаточного уровня безопасности необходимо воспользоваться рядом правил при организации и настройке частной Wi-Fi-сети:

1)максимальный уровень безопасности обеспечит применение VPN - используйте эту технологию в корпоративных сетях. И хотя технология VPN не предназначалась изначально именно для Wi-Fi, она может использоваться для любого типа сетей, и идея защитить с её помощью беспроводных их вариантов одна из лучших на сегодня. Плюс технологии состоит и в том, что на протяжении более трёх лет практического использования в индустрии данный протокол не получил никаких нареканий со стороны пользователей. Информации о его взломах не было.;

2)если есть возможность использовать 802.1X (например, точка доступа поддерживает, имеется RADIUS-сервер) - воспользуйтесь ей (впрочем, уязвимости есть и у 802.1X);

3) перед покупкой сетевых устройств внимательно ознакомьтесь с документацией. Узнайте, какие протоколы или технологии шифрования ими поддерживаются. Проверьте, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов;

4) обратите внимание на устройства, использующие WPA2 и 802.11i, поскольку в этом стандарте для обеспечения безопасности используется новый Advanced Encryption Standard (AES);

5) если точка доступа позволяет запрещать доступ к своим настройкам с помощью беспроводного подключения, то используйте эту возможность. Настраивайте AP только по проводам. Не используйте по радио протокол SNMP, web-интерфейс и telnet;

6) если точка доступа позволяет управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List),

используйте эту возможность. Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника;

7) если оборудование позволяет запретить трансляцию в эфир идентификатора SSID, используйте эту возможность (опция может называться «closed network»), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента;

8) запретите доступ для клиентов с SSID по умолчанию «ANY», если оборудование позволяет это делать. Не используйте в своих сетях простые SSID - придумайте что-нибудь уникальное, не завязанное на название вашей организации и отсутствующее в словарях. Впрочем, SSID не шифруется и может быть легко перехвачен (или подсмотрен на ПК клиента);

9) располагайте антенны как можно дальше от окон, внешних стен здания, а также ограничивайте мощность радиоизлучения, чтобы снизить вероятность подключения «с улицы». Используйте направленные антенны, не используйте радиоканал по умолчанию;

10) если при установке драйверов сетевых устройств предлагается выбор между технологиями шифрования WEP, WEP/WPA (средний вариант), WPA, выбирайте WPA (в малых сетях можно использовать режим Pre-Shared Key (PSK)). Если устройства не поддерживают WPA, то обязательно включайте хотя бы WEP. При выборе устройства никогда не приобретайте то, что не поддерживает даже 128bit WEP.

11) всегда используйте максимально длинные ключи. 128-бит - это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырёх заранее заданных ключей - сообщите клиентам о том, в какой день недели какой ключ используется).

12) не давайте никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание траффика путем внедрения в передаваемый поток - очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор;

13) если вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку - администратору;

14) обязательно используйте сложный пароль для доступа к настройкам точки доступа. Если точка доступа не позволяет ограничивать доступ паролем, её место на свалке;

15) если для генерации ключа предлагается ввести ключевую фразу, то используйте набор букв и цифр без пробелов. При ручном вводе ключа WEP вводите значения для всех полей ключа (при шестнадцатеричной записи вводить можно цифры 0-9 и буквы a-f).

16) по возможности не используйте в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае

безопаснее. Не разрешайте гостевой доступ к ресурсам общего доступа, используйте длинные сложные пароли;

17) по возможности, не используйте в беспроводной сети DHCP - вручную распределить статические IP-адреса между легитимными клиентами безопаснее;

18) на всех ПК внутри беспроводной сети установите файерволлы, старайтесь не устанавливать точку доступа вне брандмауэра, используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл стоит обычно один - на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл;

19) регулярно исследуйте уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновляйте прошивки и драйвера устройств, устанавливайте заплатки для Windows.

Лекция №15. Технология VPN и варианты построения защищенных виртуальных сетей

Цель лекций: аббревиатура VPN расшифровывается как Virtual Private Network – «виртуальная частная сеть». Суть этой технологии в том, что при подключении к VPN серверу при помощи специального программного обеспечения поверх общедоступной сети в уже установленном соединении организуется зашифрованный канал, обеспечивающий высокую защиту передаваемой по этому каналу информации за счёт применения специальных алгоритмов шифрования.

В общем случае VPN - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую виртуальную (наложенную) сеть, обеспечивающую секретность и целостность передаваемой по ней информации (прозрачно для пользователей).

Использование технологии VPN необходимо там, где требуется защита корпоративной сети от воздействия вирусов, злоумышленников, просто любопытных, а также от других угроз, являющихся результатом ошибок в конфигурировании или администрировании сети.

Виртуальные частные сети (VPN), создаваемые на базе арендуемых и коммутируемых каналов связи сетей общего пользования (и, в первую очередь, Интернет), являются отличной альтернативой изолированным корпоративным сетям, причем, альтернативой, обладающей рядом несомненных преимуществ:

- низкая стоимость арендуемых каналов и коммуникационного оборудования развитая топология сети (широкий географический охват);
- высокая надежность;
- легкость масштабирования (подключения новых сетей или пользователей);

- легкость изменения конфигурации; контроль событий и действий пользователей.

Какими свойствами должна обладать VPN?

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе сети общего пользования, в виртуальную частную сеть:

- шифрование;
- аутентификация;
- контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий. Ниже приведены примеры реализации решений путем применения технологии VPN.

При выборе средств построения защищенных виртуальных сетей необходимо учитывать такие характеристики этих средств, как функциональная полнота, надежность, гибкость, производительность, управляемость и совместимость. Обобщенные достоинства и недостатки средств создания VPN различных категорий представлены в таблице 13.1.

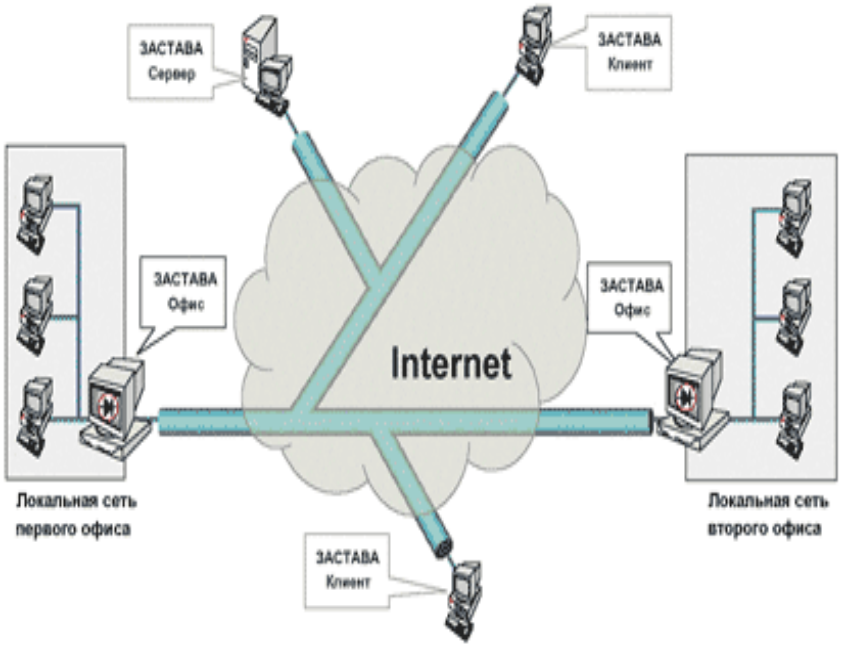

Рисунок 13.1 - пример решения, позволяющий объединить территориально разнесенные ЛВС, удаленный сервер и удаленных клиентов

Таблица 13.1 - Достоинства и недостатки средств создания VPN различных категорий

Категория	Достоинства	Недостатки
VPN на базе маршрутизаторов	Функции поддержки сетей VPN могут быть встроены в маршрутизирующие устройства, что не потребует дополнительных расходов на приобретение средств, реализующих эти функции. Упрощается администрирование VPN	Функционирование VPN может отрицательно повлиять на другой трафик. Канал между получателем информации внутри локальной сети и маршрутизатором может стать уязвимым звеном в системе защиты
Программное обеспечение VPN для брандмауэров	Возможен контроль туннелируемого трафика Достигается высокая эффективность администрирования защищённых виртуальных сетей Обеспечивается комплексная защита информационного обмена. Отсутствует избыточность аппаратных платформ для средств сетевой защиты	Операции, связанные с шифрованием данных, могут чрезмерно загружать процессор и снижать производительность брандмауэра. Если защищённый туннель завершается на брандмауэре, то канал между получателем информации внутри локальной сети и брандмауэром может стать уязвимым звеном в системе защиты. При повышении производительности серверных продуктов аппаратное обеспечение потребуется модернизировать
VPN на базе специализированного программного обеспечения	Возможность модернизации и обновления версий. Оперативность устранения ошибок. Не требуется специальных аппаратных средств	Администрирование VPN может потребовать отдельного приложения, возможно, даже выделенного каталога. При повышении производительности серверных продуктов аппаратное обеспечение может потребоваться модернизировать
VPN на базе аппаратных средств	Обеспечивается более высокая производительность. Многофункциональные аппаратные устройства облегчают конфигурацию и обслуживание. Однофункциональные аппаратные устройства допускают тонкую настройку для достижения наивысшей производительности	В многофункциональных блоках производительность одного приложения повышается зачастую в ущерб другому. Однофункциональные устройства могут потребовать отдельных инструментов администрирования и каталогов. Модернизация для повышения производительности нередко оказывается слишком дорогостоящей или невозможной. Канал между получателем информации внутри локальной сети и аппаратным устройством шифрования трафика может стать уязвимым звеном в системе защиты

Список литературы

1. Крук Б. И., Попантонопуло В.Н., Шувалов В. П.. Телекоммуникационные системы и сети. Современные технологии. Том 1. Под редакцией проф. В. П, Шувалова. - М.: Изд. «Горячая линия- Телеком», 2005. - 642 с.
2. Основы организации сетей CISCO. Том 1. - М., 2002. - 505 с.
3. М. А. Ташимов. Современные вычислительные системы и сетевые технологии. Изд. ТОО “ Print- S”. - Алматы, 2004.- 384 с.
4. Лайза Хендерсон, Том Дженкинс, Frame Relay межсетевые взаимодействия. - Москва: «Горячая линия – Телеком», 2000.
5. Гальперович Д. Широкополосный доступ по DSL. Ж. LAN, №2, 2007.
6. Иванцов И. Эволюция доступа DSL. Ж., №10, 2007.
7. Мучлер Ш. Мастера интеграции на небольшой площади. Журнал LAN, № 3, 2007.
8. Гальперович Д. Скоростной доступ в Internet. Журнал LAN, № 6, 2006
9. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа– М.: Эко-Трендз, 2005.
10. WLAN: практическое руководство для администраторов и профессиональных пользователей»/Томас Мауфер. – М.: КУДИЦ-Образ, 2005.
11. Беспроводные сети. Первый шаг / Джим Гейер. – М.: Издательство: Вильямс, 2005.
12. Секреты беспроводных технологий»/Джек Маккалоу. – М.: НТ-Пресс, 2005.
13. Современные технологии и стандарты подвижной связи»/ Кузнецов М.А., Рыжков А.Е. – СПб.: Линк, 2006.
14. Олифер В. Г., Олифер Н. А. Основы сетей передачи данных.
15. www. intuit. ru.
16. www. citforum.ru.
17. book.itep.ru

СОДЕРЖАНИЕ

Введение……...3

Лекция №1. Стандарты и технические спецификации в области информационной безопасности……4

Лекция №2. Компьютерные атаки и технологии их обнаружения ……6

Лекция №3. Этапы реализации атак ……8

Лекция №4. Криптографические средства защиты компьютерных сетей……14

Лекция №5. Вредоносное программное обеспечение (вирусы)……..18

Лекция №6. Сетевые вирусы ……...21

Лекция №7. Защита от вредоносного ПО……...25

Лекция №8. Проблемы безопасности протоколов TCP/IP……28

Лекция №9. Выявление уязвимостей компьютерных сетей……32

Лекция №10 Экранирование и межсетевые экраны……...37

Лекция №11. Защита от несанкционированного доступа……...39

Лекция №12. Безопасность электронной коммерции……40

Лекция №13Безопасность электронных платежных систем……42

Лекция №14. Безопасность Wi-Fi сетей……..43

Лекция №15. Технология VPN и варианты построения защищенных виртуальных сетей……47

Список литературы……...50

Сводный план 2014г., поз. 369

Тойгожинова Айнур Жумакановна
Тергеусизова Алия Советжановна

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Конспект лекций для студентов специальности
5В070400 – Вычислительная техника и программное обеспечение

Редактор Сластихина Л.Т.
Специалист по стандартизации Молдабекова Н.К.

Подписано в печать __.__.____.
Тираж 100 экз
Объем 3,3 уч.-изд. л.

Формат 60х84 1/16
Бумага типографская №1
Заказ ___. Цена 1650т.

Копировально-множительное бюро
Некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013, Алматы, Байтурсынова, 126