2. Лекция: Категории атак.

В лекции рассмотрены различные категории атак, даны их определения и условия для их осуществления. Коротко рассмотрен механизм проведения атак.

Во время работы компьютерных систем часто возникают различные проблемы. Некоторые - по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому будем называть такие события атаками, независимо от причин их возникновения.

Существуют четыре основных категории атак:

- атаки доступа;
- атаки модификации;
- атаки на отказ в обслуживании;
- атаки на отказ от обязательств.

Давайте подробно рассмотрим каждую категорию. Существует множество способов выполнения атак: при помощи специально разработанных средств, методов социального инжиниринга, через уязвимые места компьютерных систем. При социальном инжиниринге для получения несанкционированного доступа к системе не используются технические средства. Злоумышленник получает информацию через обычный телефонный звонок или проникает внутрь организации под видом ее служащего. Атаки такого рода наиболее разрушительны.

Атаки, нацеленные на захват информации, хранящейся в электронном виде, имеют одну интересную особенность: информация не похищается, а копируется. Она остается у исходного владельца, но при этом ее получает и злоумышленник. Таким образом, владелец информации несет убытки, а обнаружить момент, когда это произошло, очень трудно.

Определение атаки доступа

Атака доступа - это попытка получения злоумышленником информации, для просмотра которой у него нет разрешений. Осуществление такой атаки возможно везде, где существует информация и средства для ее передачи (рис. 2.1). Атака доступа направлена на нарушение конфиденциальности информации.

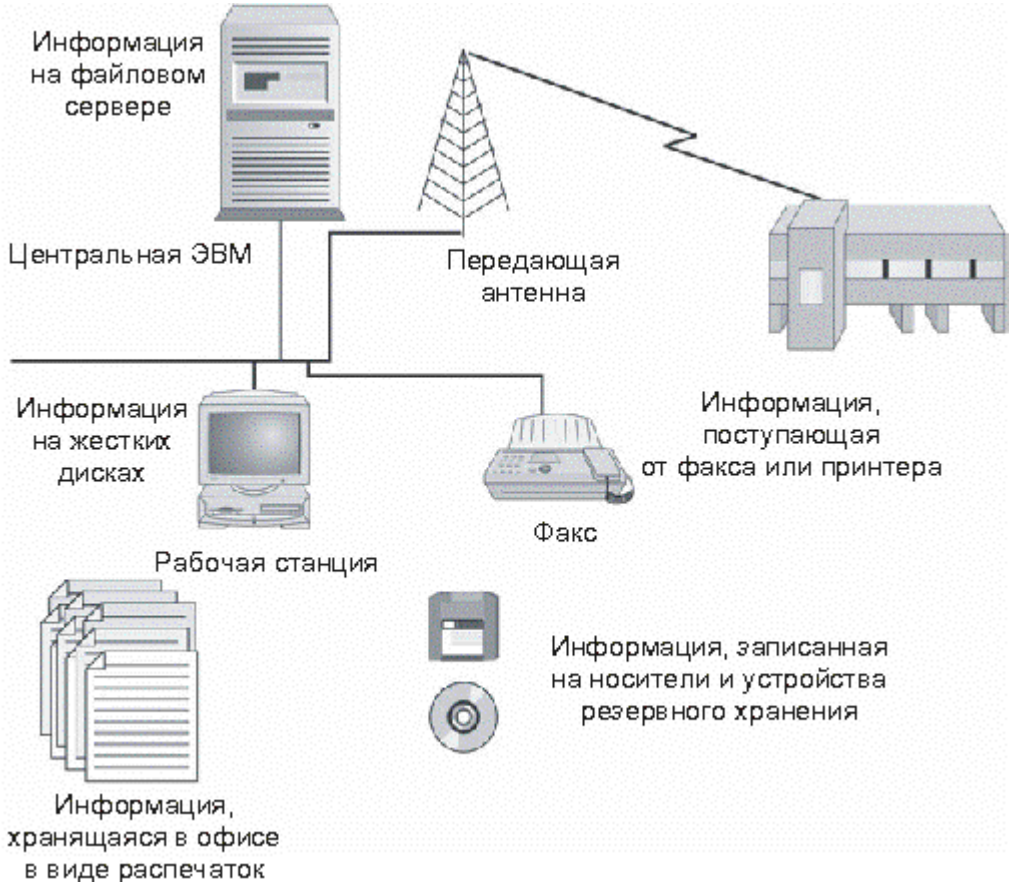

Рис. 2.1. Атака доступа возможна везде, где существуют информация и средства для ее передачи

Подсматривание

Подсматривание (snooping) - это просмотр файлов или документов для поиска интересующей злоумышленника информации. Если документы хранятся в виде распечаток, то злоумышленник будет вскрывать ящики стола и рыться в них. Если информация находится в компьютерной системе, то он будет просматривать файл за файлом, пока не найдет нужные сведения.

Подслушивание

Когда кто-то слушает разговор, участником которого он не является, это называется подслушиванием (eavesdropping). Для получения несанкционированного доступа к информации злоумышленник должен находиться поблизости от нее. Очень часто при этом он использует электронные устройства (рис. 2.2).

Внедрение беспроводных сетей увеличило вероятность успешного прослушивания. Теперь злоумышленнику не нужно находиться внутри системы или физически подключать подслушивающее устройство к сети. Вместо этого во время сеанса связи он располагается на стоянке для автомобилей или вблизи здания.

Внимание!

Появление беспроводных сетей создало многочисленные проблемы безопасности, открыв несанкционированный доступ злоумышленников к внутренним сетям. Эти проблемы будут подробно рассмотрены далее.

Рис. 2.2. Подслушивание

Перехват

В отличие от подслушивания перехват (interception) - это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. После анализа информации он принимает решение о разрешении или запрете ее дальнейшего прохождения (рис. 2.3).

Рис. 2.3. Перехват

Как выполняются атаки доступа

Атаки доступа принимают различные формы в зависимости от способа хранения информации: в виде бумажных документов или в электронном виде на компьютере.

Документы

Если необходимая злоумышленнику информация хранится в виде бумажных документов, ему потребуется доступ к этим документам. Они, возможно, отыщутся в следующих местах:

- в картотеках;
- в ящиках столов или на столах;
- в факсе или принтере;
- в мусоре;
- в архиве.

Следовательно, злоумышленнику необходимо физически проникнуть во все эти места. Если он является служащим данной организации, то сможет попасть в помещения с картотекой. Письменные столы он найдет в незапертых офисах. Факсы и принтеры обычно располагаются в общедоступных местах, и люди имеют привычку оставлять там распечатанные документы. Даже если все офисы закрыты, можно покопаться в мусорных корзинках, выставленных в холл для очистки. А вот архивы станут для взломщика проблемой, особенно если они принадлежат разработчикам и расположены в охраняемом месте.

Замки на дверях, возможно, и остановят кого-то, но всегда отыщутся помещения, оставленные открытыми на время обеда. Замки на ящиках картотеки и в столах относительно просты, их можно легко открыть отмычкой, особенно если знать, как это делается.

Физический доступ - это ключ к получению данных. Следует заметить, что надежная защита помещений оградит данные только от посторонних лиц, но не от служащих организации или внутренних пользователей.

Информация в электронном виде

Информация в электронном виде хранится:

- на рабочих станциях;
- на серверах;
- в портативных компьютерах;
- на флоппи-дисках;
- на компакт-дисках;
- на резервных магнитных лентах.

Злоумышленник может просто украсть носитель данных (дискету, компакт-диск, резервную магнитную ленту или портативный компьютер). Иногда это сделать легче, чем получить доступ к файлам, хранящимся в компьютерах.

Если злоумышленник имеет легальный доступ к системе, он будет анализировать файлы, просто открывая один за другим. При должном уровне контроля над разрешениями доступ для нелегального пользователя будет закрыт, а попытки доступа зарегистрированы в журналах.

Правильно настроенные разрешения предотвратят случайную утечку информации. Однако серьезный взломщик постарается обойти систему контроля и получить доступ к нужной информации. Существует большое количество уязвимых мест, которые помогут ему в этом.

При прохождении информации по сети к ней можно обращаться, прослушивая передачу. Взломщик делает это, устанавливая в компьютерной системе сетевой анализатор пакетов (sniffer). Обычно это компьютер, сконфигурированный для захвата всего сетевого трафика (не только трафика, адресованного данному компьютеру). Для этого взломщик должен повысить свои полномочия в системе или подключиться к сети (рис. 2.2). Анализатор настроен на захват любой информации, проходящей по сети, но особенно - на пользовательские идентификаторы и пароли.

Как уже говорилось выше, появление беспроводной технологии позволяет взломщикам перехватывать трафик без физического доступа к системе. Беспроводные сигналы считываются на довольно большом расстоянии от их источника:

- на других этажах здания;
- на автомобильной стоянке;
- на улице рядом со зданием.

Подслушивание выполняется и в глобальных компьютерных сетях типа выделенных линий и телефонных соединений. Однако такой тип перехвата требует наличия соответствующей аппаратуры и специальных знаний. В этом случае наиболее удачным местом для размещения подслушивающего устройства является шкаф с электропроводкой.

Перехват возможен даже в системах оптико-волоконной связи с помощью специализированного оборудования, обычно выполняется квалифицированным взломщиком.

Информационный доступ с использованием перехвата - одна из сложнейших задач для злоумышленника. Чтобы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и получателем информации. В интернете это выполняется посредством изменения

разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес (рис. 2.4). Трафик перенаправляется к системе атакующего вместо реального узла назначения. При соответствующей настройке такой системы отправитель так и не узнает, что его информация не дошла до получателя.

Вопрос к эксперту

Вопрос. Что вы можете рассказать о так называемом "вочокинге" (от англ. warchalking)?

Ответ. Этот термин означает нанесение мелом специальных знаков на тротуарах около зданий офисов. Такие отметки сигнализируют взломщикам о наличии поблизости беспроводных сетей. Более подробная информация находится по адресу http://www.warchalking.org/.

Перехват возможен и во время действительного сеанса связи. Такой тип атаки лучше всего подходит для захвата интерактивного трафика типа telnet. В этом случае взломщик должен находиться в том же сегменте сети, где расположены клиент и сервер. Злоумышленник ждет, когда легальный пользователь откроет сессию на сервере, а затем с помощью специализированного программного обеспечения занимает сессию уже в процессе работы. Взломщик получает на сервере те же привилегии, что и пользователь.

Рис. 2.4. При перехвате используется неправильная информация о разрешении имени

Примечание

Перехват более опасен, чем прослушивание, он означает направленную атаку против человека или организации.

Определение атаки модификации

Атака модификации - это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации

Замена

Одним из видов атаки модификации является замена существующей информации, например, изменение заработной платы служащего. Атака замены направлена как против секретной, так и общедоступной информации.

Добавление

Другой тип атаки - добавление новых данных, например, в информацию об истории прошлых периодов. Взломщик выполняет операцию в банковской системе, в результате чего средства со счета клиента перемещаются на его собственный счет.

Удаление

Атака удаления означает перемещение существующих данных, например, аннулирование записи об операции из балансового отчета банка, в результате чего снятые со счета денежные средства остаются на нем.

Как выполняются атаки модификации

Как и атаки доступа, атаки модификации выполняются по отношению к информации, хранящейся в виде бумажных документов или в электронном виде на компьютере

Документы

Документы сложно изменить так, чтобы этого никто не заметил: при наличии подписи (например, в контракте) нужно позаботиться о ее подделке, скрепленный документ необходимо аккуратно собрать заново.

Примечание

При наличии копий документа их тоже нужно переделать, как и исходный. А поскольку практически невозможно найти все копии, подделку заметить очень легко.

Очень трудно добавлять или удалять записи из журналов операций. Во-первых, информация в них расположена в хронологическом порядке, поэтому любое изменение будет сразу замечено. Лучший способ - изъять документ и заменить новым. Для атак такого рода необходим физический доступ к информации.

Информация, хранящаяся в электронном виде

Модифицировать информацию, хранящуюся в электронном виде, значительно легче. Учитывая, что взломщик имеет доступ к системе, такая операция оставляет после себя минимум улик. При отсутствии санкционированного доступа к файлам атакующий сначала должен обеспечить себе вход в систему или удалить разрешения файла. Атаки такого рода используют уязвимые места систем, например, "бреши" в безопасности сервера, позволяющие заменить домашнюю страницу.

Изменение файлов базы данных или списка транзакций должно выполняться очень осторожно. Транзакции нумеруются последовательно, и удаление или добавление неправильных операционных номеров будет замечено. В этих случаях необходимо основательно поработать во всей системе, чтобы воспрепятствовать обнаружению.

Труднее произвести успешную атаку модификации при передаче информации. Лучший способ - сначала выполнить перехват интересующего трафика, а затем внести изменения в информацию перед ее отправкой к пункту назначения.

Вопросы для самопроверки

1. Верно ли, что легче выполнить перехват, чем прослушивание?
2. Попытка вставить запись в бухгалтерскую книгу называется атакой _____.

Определение атак на отказ в обслуживании

Атаки на отказ в обслуживании (Denial-of-service, DoS) - это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. В результате DoS-атаки злоумышленник обычно не получает доступа к компьютерной системе и не может оперировать с информацией. Иначе, как вандализмом, такую атаку не назовешь.

Отказ в доступе к информации

В результате DoS-атаки, направленной против информации, последняя становится непригодной для использования. Информация уничтожается, искажается или переносится в недоступное место.

Отказ в доступе к приложениям

Другой тип DoS-атак направлен на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются. В случае успеха подобной атаки решение задач, выполняемых с помощью такого приложения, становится невозможным.

Отказ в доступе к системе

Общий тип DoS-атак ставит своей целью вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становится недоступной.

Отказ в доступе к средствам связи

Атаки на отказ в доступе к средствам связи выполняются уже много лет. В качестве примера можно привести разрыв сетевого провода, глушение радиопередач или лавинную рассылку сообщений, создающую непомерный трафик. Целью атаки является коммуникационная среда. Целостность компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает доступа к этим ресурсам.

Как выполняются атаки на отказ в обслуживании

DoS-атаки обычно направлены против компьютерных систем и сетей, но иногда их целью являются документы на бумажных носителях.

Документы

Информация на бумажных носителях является объектом для физических атак DoS. Документы нужно украсть или уничтожить, чтобы сделать непригодными для использования. Физические атаки DoS выполняются преднамеренно или происходят случайно. Злоумышленник может просто уничтожить документы, и если их копии не сохранились, то считайте информацию пропавшей. С этой же целью он может организовать поджог здания. К таким же результатам приводят и случайности: ведь пожар может возникнуть из-за повреждения проводки, а уничтожить документ служащий может по ошибке.

Информация, хранящаяся в электронном виде

Существует много способов выполнения DoS-атак, способных повредить информацию, хранящуюся в электронном виде. Ее можно удалить, а для закрепления успеха злоумышленник удалит и все резервные копии этой информации. Он может привести файл в негодность, зашифровав его и затем уничтожив ключ шифрования. Доступ к информации будет потерян, если не существует резервной копии файла.

Физическая атака DoS - это и физическое уничтожение компьютера (или его кража). Пример кратковременной атаки DoS - отключение компьютера, в результате которого пользователи лишаются доступа к своим приложениям.

Существуют атаки DoS, нацеленные непосредственно на компьютерную систему. Они реализуются через эксплоиты, использующие уязвимые места операционных систем или межсетевых протоколов.

Злоумышленникам хорошо известны и "бреши" в приложениях. С их помощью атакующий посылает в приложение определенный набор команд, который оно не в состоянии правильно обработать, в результате чего приложение выходит из строя. Перезагрузка восстанавливает его работоспособность, но на время перезагрузки работать с приложением становится невозможно.

Самый легкий способ привести в нерабочее состояние средства коммуникации - это перерезать сетевой кабель. Для такой атаки требуется физический доступ к проводке, но, как мы увидим дальше, ковш экскаватора является мощным инструментом DoS-атак.

DoS-атаки, направленные на средства связи, выполняют отправку на сайт непомерно большого трафика. Этот трафик буквально переполняет коммуникационную инфраструктуру, лишая доступа к сети легальных пользователей.

Но не все DoS-атаки являются преднамеренными, иногда случайность играет большую роль в возникновении подобных инцидентов. Экскаватор, о котором я говорил выше, может оборвать оптико-волоконную линию передачи во время выполнения своей обычной работы. Такой обрыв уже служил поводом множества DoS-инцидентов для пользователей телефонных сетей и интернета. Разработчики, тестирующие новый программный код, иногда выводили из строя большие системы, совершенно того не желая. Даже дети становятся причиной случайной DoS-атаки. Во время экскурсии по центру обработки данных ребенок будет настолько очарован мерцающими повсюду огоньками, что не удержится от соблазна нажать на красивую кнопку - и остановит или перезагрузит всю систему.

Определение атаки на отказ от обязательств

Эта атака направлена против возможности идентификации информации, другими словами, это попытка дать неверную информацию о реальном событии или транзакции.

Маскарад

Маскарад - это выполнение действий под видом другого пользователя или другой системы. Такая атака реализуется при связи через персональные устройства, при осуществлении финансовых операций или при передаче информации от одной системы к другой.

DoS-атаки против интернета

Целью DoS-атак обычно является отдельная компьютерная система или линия связи, но иногда они направлены против всего интернета! В 2002 г. произошла атака на серверы корневых имен интернета. Они были буквально "завалены" запросами на разрешение имен. Запросов было так много, что некоторые компьютеры вышли из строя. Но атака не имела полного успеха, так как многие серверы не потеряли работоспособность, и интернет продолжал функционировать. Если бы удалось вывести из строя все серверы, то интернет стал бы недоступным по большинству разрешенных имен.

Отрицание события

Отрицание события - это отказ от факта совершения операции. Например, человек делает покупку в магазине при помощи кредитной карты. Когда приходит счет, он заявляет компании, предоставившей ему кредитную карту, что никогда не делал этой покупки.

Как выполняются атаки на отказ от обязательств

Атаки выполняются по отношению к информации, хранящейся в виде бумажных документов или в электронном виде. Сложность реализации атаки зависит от мер предосторожности, принятых в организации.

Документы

Злоумышленник выдает себя за другого человека, используя чужие документы. Это легче делать, если документ напечатан, а не написан от руки.

Злоумышленник отрицает факт свершения сделки. Если на контракте или квитанции кредитной карты имеется подпись, он заявит, что это не его подпись. Естественно, планируя такую атаку, он постарается, чтобы подпись выглядела неправдоподобно.

Информация в электронном виде

Атаки на отказ от обязательств выполняются гораздо успешнее, если информация представлена в электронном виде. Ведь электронный документ может создать и отправить кто угодно. В поле "от" ("from") адреса электронной почты легко изменить имя отправителя, подлинность которого не проверяется службой электронной почты.

Это справедливо и для информации, передаваемой компьютерными системами. Система может назначить себе любой IP-адрес и замаскироваться под другую систему.

Примечание

Мы привели упрощенный пример. Система сможет назначить IP-адрес другой системы, если находится в том же самом сегменте сети. В интернете сделать подобную замену очень сложно, так как это не позволит установить подключение.

В электронной среде гораздо легче отрицать факт свершения какого-либо события, ведь на цифровых документах и квитанциях кредитной карты нет рукописной подписи.

Если документ не имеет цифровой подписи, то невозможно доказать его принадлежность определенному человеку. Но даже если подпись имеется, всегда можно сказать, что она украдена или что раскрыт пароль, защищающий ключ. Таким образом, очень трудно связать конкретного человека с конкретным событием - намного легче отрицать это.

В электронной среде легче отказаться от выполнения операции с кредитной картой, ведь на ней нет подписи, совпадающей с подписью ее владельца. Некоторые доказательства можно поискать, если товары отправлены по адресу владельца кредитной карты. А если их отправили в другое место? Как доказать, что владелец кредитной карты и есть тот человек, который купил товар?

Проект 2 Проверьте наличие уязвимых мест

Этот проект позволит выявить возможные пути атаки вашей информации или компьютерной системы. Такая атака будет использовать нечто хорошо вам знакомое: ваш дом или сферу вашего бизнеса.

Шаг за шагом

1. Проанализируйте информацию, относящуюся к вашему бизнесу и дому. Выявите самую важную.
2. Определите место хранения этой информации

3. Определите типы атак, наиболее разрушительных для вас. Продумайте вероятность атаки доступа, атаки модификации, атаки на отказ в обслуживании.
4. Продумайте способы обнаружения таких атак.
5. Выберите тот тип атаки, которая, по вашему мнению, является наиболее разрушительной, и разработайте стратегию атаки.

Выводы

Для многих коммерческих компаний наиболее секретными сведениями являются картотека персонала и информация о заработке. Не нужно забывать о покупателях - об их номерах кредитных карт и номерах социального обеспечения. Финансовые организации и организации здравоохранения также имеют секретную информацию, которая определенным образом регулируется. Просматривая информацию и продумывая возможность атаки, поставьте своей целью сделать так, чтобы она не была раскрыта. Возможно, что для вашего бизнеса важно учесть атаки модификации, отказа в обслуживании и отказа от обязательств.

Обнаружение атак - дело нелегкое. Вы можете использовать для этого электронные средства, но не пренебрегайте проблемами физической безопасности и персоналом своей организации. Обратил ли служащий компании внимание на то, что в офисе был посторонний? Заметил ли сотрудник изменение файла?

Наконец, при выработке стратегии не ограничивайтесь компьютерами и сетями. Подумайте о том, как злоумышленник может использовать физические средства для получения информации или для ее уничтожения.

Контрольные вопросы

1. Назовите основные категории атак.
2. Какой тип доступа требуется для выполнения атак доступа к документам?
3. Почему атаки перехвата выполнить труднее, чем прослушивание?
4. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток
5. Для какого типа атак эффективным инструментом является разрыв кабеля?
6. Против каких свойств информации направлена атака на отказ от обязательств?
7. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
8. Всегда ли атака модификации включает в себя атаку доступа?
9. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?

10. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?
11. К какому типу атак особенно уязвимы беспроводные сети?
12. Примером атаки какого рода является изменение заголовка электронной почты?
13. Что является целью атак на отказ в обслуживании?
14. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
15. Что является первым шагом при выполнении атаки модификации электронной информации?