РОССИЙСКАЯ ФЕДЕРАЦИЯ
ХАНТЫ-МАНСИЙСКИЙ АВТОНОМНЫЙ ОКРУГ-ЮГРА

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«СУРГУТСКИЙ ИНСТИТУТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА»

Кафедра: Наладчик компьютерных сетей

РЕФЕРАТ

По дисциплине: Информационная безопасность персональных компьютеров и компьютерных сетей

На тему:
Виды атак и методы взлома интрасетей

студента группы НКС 22-11 курса 1

_____
(Ф.И.О. студента)

Сургут
2022

Содержание

Введение

Цель предпринимаемых злоумышленниками атак на компьютеры из интрасетей, подключенные к Internet, состоит в получении доступа к их информационным и сетевым ресурсам. Примером могут быть базы данных, файл-серверы и т.п. Различные сетевые сервисы, например, telnet, электронная почта, видеоконференции и т.д. Под удаленной атакой (УА) принято понимать несанкционированное информационное воздействие на распределенную вычислительную систему (РВС), программно осуществляемое по каналам связи. Для УА можно выделить наиболее общие схемы их осуществления. Такие УА получили название типовых УА (ТУА). Тогда ТУА — это несанкционированное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой РВС.

Объектом удаленных атак могут стать следующие виды сетевых устройств:

- промежуточные устройства: ретрансляторы, шлюзы, модемы и т.п.
- оконечные устройства;
- каналы связи;

1.Классификация атак

Удаленные атаки можно разделить по следующим критериям:

- **По цели воздействия**, т.е. в зависимости от нарушения трех основных возможных свойств информации и информационных ресурсов — их конфиденциальности, целостности и доступности, плюс нарушение доступности всей системы или ее отдельных служб (пример атаки — "отказ в обслуживании";
- **По характеру воздействия**. УА делятся на пассивные и активные. Примером пассивного типа атак является, например, прослушивание каналов связи и перехват вводимой с клавиатуры информации. Примером активного типа является атака "третий посередине", когда злоумышленник может, например, подменять данные информационного обмена между двумя пользователями Internet и/или интрасети или между пользователем и запрашиваемым им сетевым сервисом, пересылаемые в обоих направлениях.
- **По условию начала осуществления воздействия** атака может быть безусловной (предпринимается злоумышленником в любом случае), или может активизироваться либо при посылке определенного запроса от атакуемого объекта (АО), либо при наступлении ожидаемого события на АО;
- **По расположению субъекта атаки относительно атакуемого объекта** атаки бывают внутрисегментными (средства взлома сети или, например, прослушивания каналов связи должны располагаться в том же сегменте сети, который интересует злоумышленника) или межсегментными (и тогда дальность расстояния от жертвы до злоумышленника не имеет значения);
- **По наличию обратной связи с атакуемым объектом** различают атаки с обратной связью или без обратной связи (такая атака называется однонаправленной);

- **По уровню эталонной модели взаимосвязи открытых систем OSI**, на котором осуществляется воздействие. Атака может реализовываться на всех семи уровнях — физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

Можно выделить пять основных и наиболее часто предпринимаемых в настоящее время типовых схем атак, т.е. ТУА:

- **Изучить логику работы сети** – получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий; в дальнейшем это позволит злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
- **Анализ сетевого трафика** (или прослушивание канала связи с помощью специальных средств – снифферов). Эта атака позволяет:
- **Перехватить поток передаваемых данных**, которыми обмениваются компоненты сетевой ОС – для извлечения секретной и идентификационной информации;
- **Подмена доверенного объекта или субъекта РВС** и передача по каналам связи сообщений от его имени с присвоением его прав доступа. Под доверенным объектом будем понимать станцию, легально подключенную к серверу; хотя в более общем смысле "доверенная" система – это система, которая достигает специфического уровня контроля за доступом к информации, обеспечивая механизм предотвращения (или определения) неавторизованного доступа.
- **Ложный объект РВС**. Он внедряется двумя способами:

    - **Навязыванием ложного маршрута из-за недостатков в алгоритмах маршрутизации** (т.е. проблем идентификации сетевых управляющих устройств), в результате чего можно попасть, на-

пример, на ПК или в сеть злоумышленника, где с помощью определенных средств можно "вскрыть" атакуемый компьютер;

- **Использованием недостатков алгоритмов удаленного поиска** (SAP (NetWare), ARP и DNS (Internet)...).

Эта атака позволяет воздействовать на перехваченную информацию следующим образом:

- Проводить селекцию и сохранение потока информации;
- Модифицировать информацию: в передаваемых данных или в передаваемом коде;
- Подменять информацию.

- **Отказ в обслуживании**. Атака может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов. В этом способе проникновения используется возможность фрагментирования пакетов, содержащаяся в спецификации IP. Нападающий передает слишком много фрагментов пакетов, которые должны быть смонтированы принимающей системой. Если общий объем фрагментов превышает максимально допустимый размер пакета, то система "зависает" или даже выходит из строя. Результатом осуществления данной атаки может стать:

  - Нарушение, работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост;
  - Передача с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может "вместить" трафик (атака — направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ПК из-за

невозможности системы заниматься ничем другим, кроме обработки запросов.

- **Удаленный контроль над станцией в сети**. Атака заключается в запуске на атакуемом компьютере программы "сетевого шпиона", основная цель которой - получение удаленного контроля над станцией в сети. Схематично основные этапы работы сетевого шпиона выглядят следующим образом: инсталляция в памяти; ожидание запроса с удаленного хоста, на котором запущена головная сервер-программа и обмен с ней сообщениями о готовности; передача перехваченной информации на головную сервер-программу или предоставление ей контроля над атакуемым компьютером.

2.Классические методы взлома интрасетей

Подбор пароля обычным методом:

Пароли при подключении интрасетей к Internet используют в двух целях:

- для аутентификации пользователей операционной системой, программным продуктом или аппаратными средствами (по паролю CMO5);
- в качестве ключа для шифрования данных.

Первая цель злоумышленника при взломе интрасети или ПК - получить доступ к системе . Основная ошибка заключается в том, что администраторы сети либо вообще отказывались использовать пароль, либо выбирали в качестве пароля чересчур простые и очевидные слова. Пароль может подбираться непосредственно на ПК пользователя или файл с паролями может переноситься на ПК злоумышленника для применения программы-подборщика паролей там.

Поскольку подбор правильного имени пользователя и комбинации паролей требует больших затрат времени, злоумышленники пишут специальные программы, чтобы автоматизировать этот процесс. Некоторые из этих программ, пытаясь получить доступ к системе, просто используют список общеупотребительных паролей с известным или установленным по умолчанию именем пользователя. Другие программы используют комбинацию сетевых утилит UNIX типа Finger (программы вывода информации о некотором пользователе), чтобы выяснить имена пользователей данной системы, и затем пробуют в качестве паролей различные перестановки символов, встречающихся в этих именах.

Подбор пароля методом «грубой силы»:

В зависимости от типа операционной системы (ОС) нападающий в первую очередь может опробовать существующие системные установки паролей по умолчанию. Если после установки системы эти значения не менялись, то система с большей долей вероятности окажется взломанной.

Во многих ОС имеются специфические имена пользователей. Например, в UNIX-системах всегда имеется пользователь root, на VMS - system, в NetWare - supervisor. Эти пользователи создаются во время инсталляции системы и являются пользователями по умолчанию. Они могут также быть созданы без пароля или с одним и тем же паролем для каждой инсталляции. Поэтому важно, чтобы их пароли были впоследствии изменены.

Хороший пример имени пользователя, задаваемого при установке системы — Administrator для Windows NT и bin для некоторых операционных систем UNIX. Хотя при обычных условиях, в случае попытки войти в систему с использованием такого имени, можно получить лишь информацию о версии операционной системы, некоторые реализации FTP позволяют пользователю с именем bin прочитать файл паролей.

Злоумышленник может также попробовать войти в систему с гостевым паролем: guest, demo, visitor и т.п.

Подбор пароля методом «зашифровать и сравнить»:

В системе UNIX пароль и другая специфическая информация о пользователе хранится в каталоге /etc в файле, который по умолчанию доступен всем пользователям системы. Непосредственно пароли хранятся в зашифрованном виде, и для их расшифровки может потребоваться неопределенное количество часов вычислительной работы. Зная это, многие злоумышленники используют компьютерную программу, которая подбирает пароли при помощи методики, названной "зашифровать и сравнить". Суть метода заключается в шифровании различных слов при помощи того же са-

мого алгоритма, которым шифруются действительные пароли, а затем - в сравнении двух зашифрованных строк. Если обнаружится их соответствие, то необходимый пароль найден.

Социальная инженерия:

Злоупотребление доверием пользователей, или социальная инженерия - один уз наиболее эффективных методов получать информацию у ничего не подозревающих пользователей особенно больших корпораций, где многие пользователи даже не знают персонал своих компьютерных подразделений в лицо, общаясь в основном по телефону. Это профессионально выполняемая имитация системных администраторов, персонала телефонных компаний. Просто перебирая произвольные отделы компании, злоумышленник - подставное лицо - может получить всю необходимую информацию, чтобы войти в ее компьютерную сеть.

3.Современные методы взлома интрасетей

Выделяют четыре вида наиболее часто используемых методов взлома интрасетей и НСД к секретной информации:

1) перехват данных при их перемещении по каналам связи или при вводе с клавиатуры;
2) мониторинг в системе X Window;
3) подмена системных утилит;
4) нападения с использованием сетевых протоколов.

- **Перехват данных при их перемещении по каналам связи или при вводе с клавиатуры:**

Обмен данными по протоколу Ethernet подразумевает посылку пакетов всем абонентам одного сегмента интрасети. Заголовок пакета содержит адрес узла-приемника. Предполагается, что только узел с соответствующим адресом может принять пакет. Однако, если какой-то ПК в интрасети принимает все проходящие пакеты, независимо от их заголовков, то говорят, что она находится в promiscuous mode (смешанном режиме). Для злоумышленника не сложно перевести один из ПК подсети в promiscuous mode (предварительно получив на ней права root) и, вытягивая и анализируя пакеты, проходящие по каналам связи, получить пароли к большинству компьютеров интрасети.

В одном из наиболее распространенных методов перехвата данных при их перемещении по линиям связи в интрасети используется средство — сетевой анализатор или средство инспекции потоков данных, называемое sniffer ("ищейка"). Даже если потенциальный злоумышленник не имеет доступа к некоторому компьютеру, он может перехватить данные,

посылаемые ему, в момент их прохождения по кабелю, который подключает данный компьютер к сети. Компьютер, подключенный к сети, аналогичен телефонному аппарату, подключенному к общему номеру. Любой человек может поднять трубку и подслушать чужой разговор. В случае передачи данных любой компьютер, соединенный с сетью, способен принимать пакеты, посылаемые другой станции. Главная проблема sniffer заключается в том, чтобы он успевал перерабатывать весь трафик, который проходит через интерфейс. Также есть возможность запустить sniffer в режиме non-promiscuous, но тогда будет возможность перехватывать соединения только с тем ПК, на котором он запущен.

Для перехвата символов с клавиатуры существуют многочисленные утилиты, позволяющие контролировать все символьные строки, вводимые на выбранном злоумышленником в качестве жертвы компьютере. Некоторые из них встроены в утилиты контроля данных, посылаемых с хоста во время сеансов FTP или Telnet, а другие буферизируют все символьные строки, вводимые с различных терминалов, связанных с хостом. Для ПК имеются многочисленные программы, которые выполняют те же самые функции, наблюдая за вводом с клавиатуры и сохраняя символьные строки в файл. Есть такие программы, которые никак себя не проявляют на компьютере-жертве, однако сохраняют весь ввод клавиатуры в скрытом файле.

- **Мониторинг в системе:**

На многих ПК с ОС UNIX используется графический интерфейс, известный как X Window (иначе называемая X11). Он позволяет пользователю легко выполнять несколько приложений и переходить с одного на другое. Пользователь начинает X-сессию, соединяясь с X-сервером и указывая, что данные должны посылаться на определенный терминал. Это может быть как системная консоль, так и любой другой терминал, соединенный с сервером. Взаимодействие X-клиента и X-сервера происходит

в рамках протокола прикладного уровня - X-протокола. X-сервер представляет собой отдельный UNIX-процесс. Он общается с программами-клиентами, посылая им или принимая от них пакеты данных. Если сервер и клиент находятся на разных ПК, то данные пересылаются по сети, а если на одном, то используется внутренний канал.

X Window обеспечивает два различных механизма аутентификации:

1) механизм аутентификации хостов позволяет определить, с какого компьютера приложения могут соединяться с X-сервером, т.е. заранее определяется список доверенных ПК;

2) механизм аутентификации пользователей позволяет определить пользователей, имеющих доступ к X-серверу.

По своей природе система X Window недостаточно защищена от перехвата данных. Имеется ряд проблем с X Window, включая возможности для нападающих блокировать доступ к серверу, выполнять на нем нежелательные команды и перехватывать ввод, сгенерированный на сервере. При помощи простой программы, доступной в хакерской среде, все нажатия клавиш в некоторой сессии X Window могут быть перехвачены и сохранены в файл. Предположим, что пользователь работает на рабочей станции-клиенте. В сети существует сервер, на котором этот пользователь хочет выполнять свои приложения вместо того, чтобы выполнять их на локальной рабочей станции. В X Window это легко сделать, задавая определенные параметры или устанавливая переменную среды DISPLAY. Для этого пользователь сначала должен разрешить приложениям, выполняющимся на сервере, соединяться с его X-сервером.

- **Подмена системных утилит:**

В прошлом модификации системных утилит ограничивались программой login, в которую нападающий мог запрограммировать некоторый

свой пароль, предоставляющий ему неограниченный доступ к системе в любое время. Сегодня тот же метод применяется в отношении других утилит идентификации, существующих в Internet и интрасетях. Широкая доступность исходного текста утилит системы UNIX еще более упростила этот процесс, поскольку злоумышленник может легко найти текст нужной ему утилиты и модифицировать ее по своему усмотрению. Некоторые из лучших подделок даже компилируют до точного совпадения размера в байтах с исходной версией. Кроме традиционного "черного входа", многие подделки позволяют пользователю скрываться от программы учета процессов. Поскольку злоумышленник входит в систему через "черный вход", его присутствие не фиксируется в системных файлах регистрации.

В среде UNIX имеются многочисленные системные файлы регистрации, которые следят за событиями типа некорректных попыток входа в систему, нормальных входов в систему и выходов из нее, а также за выполняемыми командами. Файл UTMP следит за всеми пользователями, в текущий момент зарегистрированными в системе. WTMP или lastlog, следит за временем входа в систему и выхода из нее. Базы данных регистрации процессов, обычно называемые acct или pacct, следят за всеми командами, выполняемыми отдельными пользователями. Если модифицировать эти файлы, пользователь останется невидимым для команд типа who, last и lastcomm. Этот тип модификации, дополненный определенными утилитами, значительно затрудняет администратору системы установление факта атаки со стороны злоумышленника.

- **Нападение и использованием сетевых протоколов:**

Много угроз несет с собой передача специальных пакетов, которые либо содержат неверную информацию, либо были преднамеренно искажены. Пакеты стандарта TCP/IP имеют специфический порядок байтов, размер и строго определенные поля. В большинстве случаев неправильно

составленный пакет будет игнорироваться и отрабатываться либо сетевым интерфейсом, либо маршрутизатором где-нибудь на пути от источника пакета к адресату.

Активные атаки можно разделить на две части. В первом случае злоумышленник предпринимает определенные шаги для перехвата и модификации сетевого потока или попыток "притвориться" другой системой. Во втором случае протокол TCP/IP используется для того, чтобы привести систему-жертву в нерабочее состоянии. Обладая достаточными привилегиями в UNIX (или попросту используя DOS или Windows, не имеющие системы ограничений пользователей), злоумышленник может вручную формировать IP-пакеты и передавать их по сети. Поля заголовка пакета могут быть сформированы произвольным, образом. Получив такой пакет, невозможно выяснить откуда реально он был получен, поскольку пакеты не содержат пути их прохождения.

Источники:

1. https://moluch.ru/conf/tech/archive/5/1115/
2. https://studfile.net/preview/9124450/page:182/
3. https://studfile.net/preview/9124450/page:180/
4. https://studfile.net/preview/9124450/page:183/
5. https://www.internet-technologies.ru/articles/newbie/klassifikaciya-setevyh-atak.html