Варданян Наира Андраниковна
учитель информатики
Государственное бюджетное образовательное учреждение города Москвы
средняя общеобразовательная школа № 1980
г. Москва

АНАЛИЗ УГРОЗ СЕТЕВОЙ БЕЗОПАСНОСТИ

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP/IP, обеспечивающий совместимость между компьютерами разных типов. Совместимость - одно из основных преимуществ TCP/IP, поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. Создавая свое детище, архитекторы стека TCP/IP не видели причин особенно беспокоиться о защите сетей, строящихся на его основе. Поэтому в спецификациях ранних версий протокола IP отсутствовали требования безопасности, что привело к изначальной уязвимости его реализации.

Проблемы безопасности IP-сетей

Стремительный рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т.д.

Характерные особенности сетевых атак

Каждый день хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных

атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. Сегодня к этой сети подключены миллионы компьютеров. Многие миллионы компьютеров будут подключены к Интернету в ближайшем будущем, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании операционных систем и сред разработки. Этот фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

Проблемы обеспечения информационной безопасности в корпоративных компьютерных сетях обусловлены угрозами безопасности для локальных рабочих станций, локальных сетей и атаками на корпоративные сети, имеющие выход в общедоступные сети передачи данных.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие способен осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность.

Нарушитель, осуществляя атаку, обычно ставит перед собой следующие цели:

- нарушение конфиденциальности передаваемой информации;
- нарушение целостности и достоверности передаваемой информации;
- нарушение работоспособности системы в целом или отдельных ее частей.

С точки зрения безопасности распределенные системы характеризуются, прежде всего, наличием ***удаленных атак,*** поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности, поскольку препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Безопасность локальной сети по сравнению с безопасностью межсетевого взаимодействия отличается тем, что в этом случае на первое по значимости место выходят ***нарушения зарегистрированных пользователей,*** поскольку в основном каналы передачи данных локальной сети находятся на контролируемой территории и защита от несанкционированного подключения к ним реализуется административными методами.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например, с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется**.**

Рассмотрим наиболее распространенные виды сетевых атак.

Подслушивание (sniffing). По большей части данные по компьютерным сетям передаются в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в вашей сети, подслуши-

вать или считывать трафик. Для подслушивания в компьютерных сетях используют **сниффер.** ***Сниффер пакетов*** представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако, ввиду того что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват пароля (password sniffing), передаваемого по сети в незашифрованной форме, путем «подслушивания» канала является разновидностью атаки подслушивания. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает атрибуты нового пользователя, которые можно в любой момент использовать для доступа в сеть и к ее ресурсам.

Предотвратить угрозу сниффинга пакетов можно с помощью следующих мер и средств:

- применение для аутентификации однократных паролей;
- установка аппаратных или программных средств, распознающих снифферы;
- применение криптографической защиты каналов связи.

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг - изменить их. Данные в пакете

могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе. Даже если вы не нуждаетесь в строгой конфиденциальности всех передаваемых данных, наверняка вы не захотите, чтобы они были изменены по пути.

Анализ сетевого трафика. Целью атак подобного типа являются прослушивание каналов связи и анализ передаваемых данных и служебной информации с целью изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде). Атакам данного типа подвержены такие протоколы, как FTP или Telnet, особенностью которых является то, что имя и пароль пользователя передаются в рамках этих протоколов в открытом виде.

Подмена доверенного субъекта. Большая часть сетей и операционных систем использует IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом) - такой способ атаки называют ***фальсификацией адреса*** **(IP-spoofing).**

Посредничество. Атака типа «посредничество» подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определить, с кем именно они обмениваются данными.

Перехват сеанса (Session hijacking). По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например, с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети у атакующего злоумышленника

появляются большие возможности:

- он может посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;
- он может также наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в связи с перегрузкой;
- наконец, атакующий может блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

Отказ в обслуживании (Denial of Service, DoS). Эта атака отличается от атак других типов. Она не нацелена на получение доступа к вашей сети или на извлечение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Парольные атаки. Целью этих атак является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как:

- подмена IP-адреса (1P-спуфинг);
- подслушивание (сниффинг);
- простой перебор.

IP-спуфинг и сниффинг пакетов были рассмотрены выше. Эти методы позволяют завладеть паролем и логином пользователя, если они передаются открытым текстом по незащищенному каналу.

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа тяжело и требуются большие затраты ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована

специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется скомпрометированным. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

Атаки на уровне приложений. Эти атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании известных слабостей серверного программного обеспечения (FTP, HTTP, Web-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран.

Сетевая разведка - это сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома.

Для защиты от указанных вредоносных программ необходимо применение ряда мер:

- исключение несанкционированного доступа к исполняемым файлам;
- тестирование приобретаемых программных средств;
- контроль целостности исполняемых файлов и системных областей;
- создание замкнутой среды исполнения программ.

Литература:

Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. «Защита информации в сети – анализ технологий и синтез решений». М.: ДМК Пресс, 2004.