УДК 004.056

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В МУЛЬТИСЕРВИСНЫХ СЕТЯХ

Байгозина А.В., Баранов А.А.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua

В тезисах приведено исследование основных механизмов реализации сетевых атак в мультисервисных сетях (МС). Рассмотрены пассивные и активные воздействия на МС, последствия релизации атак, цель воздействия атак.

Ключевые слова – сетевая атака; мультисервисные сети; механизмы реализации атак; анализ сетевого трафика; подмена доверенного объекта или субъекта; ложный объект мультисервисной сети.

ВСТУПЛЕНИЕ

Можно разделить действия злоумышленников в МС на: активные и пассивные. К пассивным действиям можно отнести не только анализ сетевого трафика при подготовке атак, но и кража коммерческой или конфиденциальной информации, передаваемой по сети в виде файлов или потоков. В случае приложений потокового вещания предусматриваются меры защиты от несанкционированного копирования и нарушения, из-за кражи контента, авторских прав контентодержателя, но далеко не всегда этот вид услуг защищен от несанкционированного подслушивания/подсматривания без сохранения потока (злоумышленник аналогичен безбилетному зрителю в кинотеатре или в концертном зале).

К активным воздействиям относятся модификация или подмена информации, а также порождение паразитной сетевой информации с целью понижения или полной утраты работоспособности узлов МС.

ОСНОВНАЯ ЧАСТЬЯ

Целенаправленной атаке всегда предшествует разведка или анализ уязвимых мест сети. Поэтому необходимо пранализировать какие же существуют основные механизмы для реализации атак в мультисервисных сетях (МС):

Анализ сетевого трафика. Позволяет изучить логику работы. Удается получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы распределенной информационной системы позволяет на практике моделировать и осуществлять удаленные атаки.

Атака данного типа заключается в получении на удаленном объекте НСД к информации, которой обмениваются два сетевых абонента. При этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети

Подмена доверенного объекта или субъекта. В случае, когда в МС используются нестойкие алгоритмы идентификации объектов, оказывается возможной удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта МС. При этом существует две разновидности данной атаки с установленным виртуальным каналом или без него.

В случае установленного виртуального соединения атака будет заключаться в присвоении прав доверенного субъекта взаимодействия, легально подключившегося к объекту системы, что позволит атакующему вести сеанс работы с объектом распределенной системы от имени доверенного субъекта. Реализация удаленных атак данного типа обычно состоит в передаче, с атакующего объекта на цель атаки, пакетов обмена от имени доверенного субъекта взаимодействия. При этом переданные сообщения будут восприняты системой как корректные. Для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сообщений, которая, в принципе, может использовать контрольную сумму, вычисляемую с помощью открытого ключа, динамически выработанного при установлении канала, случайные многобитные счетчики пакетов и сетевые адреса станции.

Для служебных сообщений в МС часто используется передача одиночных сообщений, не требующих подтверждения, то есть не требуется создание виртуального соединения. Атака без установленного виртуального соединения заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, сообщения от имени маршрутизаторов).

Очевидно, что в этом случае для идентификации пакетов возможно лишь использование статистических ключей, определенных заранее, что довольно неудобно и требует сложной системы управления ключами. Однако, при отказе от такой системы идентификация пакетов без установленного виртуального канала будет возможна лишь по сетевому адресу отправителя, который легко подделать [1].

Ложный объект МС. Может быть реализован двумя путями:

- *Внедрение ложного объекта путем навязывания ложного маршрута*. Основная цель атаки, связанной с навязыванием ложного маршрута состоит в том, чтобы изменить исходную маршрутизацию на объекте МС так, чтобы новый маршрут проходил через ложный объект – хост

атакующего. Реализация данной типовой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Она часто применяется в среде IP, но мало вероятна для ATM, имеющей централизованную систему управления сетью и виртуальные каналы канального уровня. Для изменения маршрутизации атакующему злоумышленнику необходимо послать по IP-сети специальные служебные сообщения. Сделать это он может от имени сетевых управляющих устройств. Служебные сообщения определенны протоколами управления сетью. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта МС и атака перейдет во вторую стадию, связанную с приемом объектов МС.

- *Внедрение в МС ложного объекта путем использования недостатков алгоритмов удаленного поиска.* В случае использования механизмов удаленного поиска существуют возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий объект. В дальнейшем весь поток информации будет приходить через ложный объект МС. Другой вариант внедрения ложного объекта использует недостатки алгоритма удаленно поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. Атакующему, для того чтобы послать ложный ответ, не всегда обязательно дожидаться приема запроса (он может в принципе, не иметь подобной возможности перехвата запроса). При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса, и тогда его ложный ответ будет иметь немедленный успех [2].

Проанализировав основные механизмы реализации атак в МС, было выявленно на какую информацию они воздействуют в МС. Данные представленны в таблице 1.

Таблица 1. Цель воздействия сетевых атак на МС

Атака	**Цель воздействия**
Анализ сетевого трафика	Нарушение конфиденциальности информации
Подмена доверенного объекта или субъекта	Нарушение целостности, конфиденциальности информации
Внедрение ложного объекта путем навязывания ложного маршрута	Нарушение конфиденциальности, целостности или работоспособности
Внедрение в МС ложного объекта путем использования недостатков алгоритмов удаленного поиска	Нарушение целостности, конфиденциальности информации

ВЫВОД

Все вышеперечисленные механизмы атаки могут привести к таким последствиям.

При релизации атаки «Анализ сетевого трафика», производится нарушение конфиденциальности, что может привести к утечки такой информации как: имя и пароль пользователя, пересылаемое в незашифрованном виде по сети; шифрованный информационный поток для сохранения на ПК взломщика и последующего дешифрования; «подслушивание» чужих аудио- или видео потоков при недостаточной проработке защиты от мошенничества этих услуг.

При реализации атаки «Подмена доверенного объекта или субъекта» посылка ложных управляющих сообщений может привести к серьезным нарушениям работы МС (например, к изменению ее конфигурации).

«Ложный объект МС» атака, которая чрезвычайно характерна для глобальных сетей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гургенидзе А.Т., Кореш В.И. «Мультисервисные сети и услуги широкополосного доступа» / Наука и Техника, 2003. – 400 с.

2. Информационная безопасность компьютерных систем и сетей, В.Ф. Шаньгин / Москва,2008.