КЛАССИФИКАЦИЯ УДАЛЕННЫХ АТАК НА РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

1. По характеру воздействия

- пассивное
- активное

2. По цели воздействия

- нарушение конфиденциальности информации либо ресурсов системы
- нарушение целостности информации
- нарушение работоспособности (доступности) системы

3. По условию начала осуществления воздействия

- атака по запросу от атакуемого объекта
- атака по наступлению ожидаемого события на атакуемом объекте
- безусловная атака

4. По наличию обратной связи с атакуемым объектом

- с обратной связью
- без обратной связи (однонаправленная атака)

5. По расположению субъекта атаки относительно атакуемого объекта

- внутрисегментное
- межсегментное

6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

- физический
- канальный
- сетевой
- транспортный
- сеансовый
- представительный
- прикладной

ХАРАКТЕРИСТИКА И МЕХАНИЗМЫ РЕАЛИЗАЦИИ ТИПОВЫХ УДАЛЕННЫХ АТАК

Типовая удаленная атака **-** это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной ВС.

1) Анализ сетевого трафика - прослушивании канала связи

Позволяет:

во-первых, изучить логику работы распределенной ВС

во-вторых, перехватить поток данных, которыми обмениваются объекты распределенной ВС.

По характеру воздействия анализ сетевого трафика является пассивным воздействием. Осуществление данной атаки без обратной связи ведет к нарушению конфиденциальности информации внутри одного сегмента сети на канальном уровне OSI. При этом начало осуществления атаки безусловно по отношению к цели атаки.

2) Подмена доверенного объекта или субъекта распределенной ВС

- атака при установленном виртуальном канале
- атака без установленного виртуального канала.

Подмена доверенного объекта РВС является:

- активным воздействием,
- совершаемым с целью нарушения конфиденциальности и целостности информации,
- по наступлению на атакуемом объекте определенного события
- может являться как внутрисегментной, так и межсегментной
- как с обратной связью, так и без обратной связи с атакуемым объектом
- осуществляется на сетевом и транспортном уровнях модели OSI.

3) Ложный объект распределенной ВС

а) внедрение в распределенную ВС ложного объекта путем навязывания ложного маршрута

Управляющие протоколы, позволяют:
- обмениваться информацией между маршрутизаторами - (RIP (Routing Internet Protocol)),
- уведомлять хосты о новом маршруте - ICMP (Internet Control Message Protocol)),
- удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)).

Основная цель атаки, связанной с навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте распределенной ВС 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.

Навязывание объекту РВС ложного маршрута:
- активное воздействие,
- совершаемое с любой из целей из класса 2,
- безусловно по отношению к цели атаки,
- может осуществляться как внутри одного сегмента, так и межсегментно,
- как с обратной связью, так и без обратной связи с атакуемым объектом
- на транспортном и прикладном уровне модели OSI.

б) внедрение в распределенную ВС ложного объекта путем использования недостатков алгоритмов удаленного поиска

Для получения подобной информации в распределенных ВС используются различные *алгоритмы удаленного поиска*, заключающиеся в передаче по сети специального вида поисковых запросов, и в ожидании ответов на запрос с искомой информацией (ARP- и DNS-запрос в сети Internet).

Существует возможность:

- на атакующем объекте *перехватить посланный запрос и послать на него ложный ответ*, где указать данные, использование которых приведет к адресации на атакующий ложный объект.

- *периодической передаче на атакуемый объект заранее подготовленного ложного ответа* без приема поискового запроса.

- активное воздействие;
- совершаемое с целью нарушения конфиденциальности и целостности информации;
- может являться атакой по запросу от атакуемого объекта, а также безусловной атакой;
- является как внутрисегментной, так и межсегментной;
- имеет обратную связь с атакуемым объектом;
- осуществляется на канальном и прикладном уровнях модели OSI.

Использование ложного объекта для организации удаленной атаки на распределенную ВС

1. Селекция потока информации и сохранение ее на ложном объекте РВС

2. Модификация информации

a) модификация передаваемых данных;

b) модификация передаваемого кода.

- внедрение РПС (разрушающих программных средств);
- изменение логики работы исполняемого файла.

3. Подмена информации

Отказ в обслуживании

Результат применения этой удаленной атаки - нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов РВС - отказ в обслуживании!

Методы:

1. Если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то атакующий передает с одного адреса такого количества запросов на атакуемый объект, какое позволит трафик (направленный "шторм" запросов).

2. Если в распределенной ВС не предусмотрено средств аутентификации адреса отправителя, то атакующий передает на атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов,
3. Использование компьютеров-«зомби»

4. Передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы

Типовая удаленная атака "Отказ в обслуживании»:

- является активным воздействием ;
- осуществляется с целью нарушения работоспособности системы;
- безусловна относительно цели атаки;
- является однонаправленным воздействием как межсегментным, так и внутрисегментным;
- осуществляется на транспортном и прикладном уровнях модели OSI.