

25. Типовые удалённые атаки в Интернет и механизмы их реализации.

Типовые уязвимости, позволяющие организовать удаленные атаки

Компьютерные сети проектируются (и создаются) на основе одних и тех же принципов, правил (шаблонов) и, следовательно, имеют практически одинаковые проблемы безопасности в сетевых информационных системах и можно ввести понятие типовой удаленной атаки.

Типовая удаленная атака – это удаленное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной системы.

Распределённая система — система, для которой отношения местоположений элементов (или групп элементов) играют существенную роль с точки зрения функционирования системы, а, следовательно, и с точки зрения анализа и синтеза системы.

Типовые удаленные атаки и механизмы их реализации.

Удаленные угрозы можно классифицировать по следующим признакам:

- По характеру воздействия:
 - пассивные (класс 1.1);
 - активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности.

Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности.

Практически все типы удаленных угроз являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало.

Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (просмотр чужого сообщения ничего не меняет).

- По цели воздействия:
 - нарушение конфиденциальности информации (класс 2.1);
 - нарушение целостности информации (класс 2.2);
 - нарушение доступности информации (работоспособности системы) (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз — раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников — получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации.

Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения.

Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта.

Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой нарушение целостности информации, может служить типовая удаленная атака «Ложный объект распределенной вычислительной сети».

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации.

Его основная цель — добиться, чтобы узел сети или какой-то из сервисов поддерживаемый им вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака «Отказ в обслуживании».

- По условию начала осуществления воздействия

Удаленное воздействие, так же, как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

- атака по запросу от атакуемого объекта (класс 3.1);
- атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
- безусловная атака (класс 3.3).

В первом случае, злоумышленник ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS — запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае, злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

- По наличию обратной связи с атакуемым объектом:

- с обратной связью (класс 4.1);
- без обратной связи (однаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а, следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однаправленной удаленной атакой. Примером однаправленных атак является типовая удаленная атака «отказ в обслуживании».

- По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1);
- межсегментное (класс 5.2).

Рассмотрим ряд определений:

Субъект атаки (или источник атаки) — это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) — устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) (в терминологии Internet) — совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети — физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся.

В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

По уровню модели ISO/OSI, на котором осуществляется воздействие:

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).

Сетевая модель OSI — сетевая модель стека (магазина) сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99). Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Модель OSI				
Уровень (layer)		Тип данных	Функции	Примеры
Host layers	7. Прикладной (application)	Данные	Доступ к сетевым службам	HTTP, FTP, POP3
	6. Представительский (представления) (presentation)		Представление и шифрование данных	ASCII, EBCDIC
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP
	4. Транспортный (transport)	Сегменты (segment) / Дейтаграммы (datagram)	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, PORTS

Media layers	3. Сетевой (network)	Пакеты(packet)	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk
	2. Канальный (data link)	Биты (bit)/ Кадры (frame)	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP, L2 TP, сетевая карта.
	1. Физический (physical)	Биты (bit)	Работа средой передачи, сигналами и двоичными данными	USB, кабель ("витая пара", коаксиальный, оптоволоконный), радиоканал

Удаленная атака "анализ сетевого трафика"

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена.

Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого анализом сетевого трафика.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
- перехватить поток данных, которыми обмениваются объекты сети, т. е. удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

