Санкт-Петербургский Государственный Электротехнический Университет
"ЛЭТИ"им.Ульянова(Ленина).

Кафедра автоматизированных средств обработки информации и управления.

Отчет по преддипломной практике

Выполнил: Андрианов К.С.
Факультет: КТИ
Группа: 7361

Санкт-Петербург
2012

Введение.

В современном мире средства вычислительной техники широко используются во многих отраслях деятельности человека. Основной их задачей является обработка и хранение информации создаваемой пользователями или поступающей из вне. Такие системы должны обеспечивать доступ к данным и гарантировать их актуальность. Для решения проблемы быстрого получения информации конечным пользователям, отдельные компьютеры объединяются в локальные сети. Подобное объединение можно проследить вплоть до глобальной сети интернет. Однако, решив проблему, связанную с доступностью информации, соединение компьютеров обострило проблемы связанные с безопасностью данных. В случае с локальной машиной не имеющей активного сетевого соединения проблема безопасности решается ограничение физического доступа к терминалу, однако объединив рабочие станции, зона, которую необходимо контролировать, резко возрастает. Кроме того, с внедрением беспроводных технологий, это зона не имеет четких границ, а существующее подключение сети к интернет открывает потенциальную возможность для атаки человеку из любой точки мира.

Основным назначение вычислительных сетей является обмен данными между отдельными терминалами. Технология "Клиент-Сервер"позволяет передать часть нагрузки, связанной с обработкой и хранением данных, с локальной машины на сервер. Существуют так же технологии, позволяющие совместно использовать ресурсы нескольких терминалов для решения одной задачи, или же обмениваться информацией внутри сети, фактически создавая только соединения точка-точка(P2P networks).

Для рассмотрения алгоритмов, используемых при передачи данных по сети, можно воспользоваться эталонной моделью взаимодействия открытых систем. Данная модель выделяет семь уровней абстракции при обработке данных. Протоколы физического уровня определяют порядок передачи импульсов по проводнику(витая пара, оптоволокно) в соответствии с закодированными сообщениями. Канальный уровень оперирует данными с точки зрения понятия фрейма. На данном уровне рассматриваются разные типы коммутации. И разные способы передачи данных(синхронная, асинхронная - датаграммная). Адрес используемый на данном уровне - физический (MAC - адрес). На сетевом уровне определяется понятие пакета данных, использование условных адресов. Устройства коммутации в сети, такие как маршрутизаторы, обладают алгоритмами данного уровня, которые позволяют строить маршрутные таблицы для более эффективной передачи пакетов. Транспортный уровень характеризуется тем, что на данном уровне уже не используется понятие - адрес. Операции на данном уровне происходят только уровне портов взаимодействующих устройств, которые открывают сеанс и передают данные. Преобразования данных, выполняемые протоколами нижних уровней являются полностью прозрачными.

Протоколы, используемые на каждом из уровней модели могут быть подвержены ошибками и могут стать причиной некорректной передачи данных, несвоевременной их доставки или предоставить возможность злоумышленнику некоторым образом воздействовать на данные или поведение системы. Учитывая количество и сложность используемых алгоритмов, а так же разнообразие возможных способов построения и конфигурирования сетей, предусмотреть заранее все нюансы поведения той или иной части системы при возможной атаке не представляется возможным. Для оценки реакции системы на различные ситуации используется аппарат моделирования.

Целью дипломного проекта является построение системы моделирования атак на компоненты вычислительной сети.

Объектом исследования является процесс моделирования систем.

Предметом исследования является процесс моделирования атак с использованием компьютерной сети.

Моделирование атак в вычислительной сети.

Моделирование компьютерных сетей применяется для решения задач, связанных с разработкой архитектуры сети, выбора необходимых устройств, конфигурирование параметров компонентов таким образом, чтобы обеспечить наилучшие быстродействие и безопасность. При создании системы для моделирования вычислительной сети, разработчик сталкивается с рядом проблем, а именно: моделирование трафика, генерируемого пользователями, участвующими в сетевом взаимодействии, моделирование передачи физических сигналов и ошибок передачи данных, происходящих в каналах связи. В случае моделирование трафика обычно используются генераторы случайных чисел характеризующиеся равномерным или нормальным распределением.

Для моделирование события возникновения ошибки так же применяются генераторы случайных чисел с различными параметрами.

Для моделирования взаимодействия компонентов в сети могут быть использованы несколько методов. Например, использование для решения поставленной задачи раскрашенных сетей Петри. В данном случае представлением вычислительной сети является двудольным ориентированным графом. Сети Петри используются для моделирования асинхронных систем, функционирующих как совокупность параллельно взаимодействующих процессов. Сети Петри являются мощным аппаратом для моделирования процессов в вычислительной сети, однако обладают недостаточной наглядностью.

Необходимую наглядность обеспечивает метод агентно-ориентированного моделирования, являющийся видом имитационного моделирования. При таком подходе каждый компонент сети представляется в виде самостоятельной сущности. Производится описание алгоритмов его работы и взаимодействия с другими сущностями.

При моделировании атак с использованием компьютерной сети выделяют несколько главных действий, которые должен совершить злоумышленник, чтобы достичь своей цели.

- Сбор информации.

  Успех любой атаки зависит от способности злоумышленника собрать информацию о системе, на которую направлена атака. Такая информация может включать в себя IP адреса устройств, используемые операционные системы и доступные сервисы.

- Атака и проникновение.

  Используя данные, полученные на предыдущей фазе, атакующий эксплуатирует найденные уязвимости для получения доступа к системе. Например создает код, который исполняет на целевой системе, предоставляющей такую возможность.

- Сбор информации с точки зрения полученных в системе привилегий.

  Атакующий изучает параметры конфигурации операционной системы, сетевых протоколов, установленных приложениях, файлы на скопрометированной системе.

- Повышение привилегий.

  Для этого атакующий используют локальные уязвимости на терминале, к которому он получил доступ.

- Развертывание.

На данной стадии атакующий использует полученный доступ для различных действий, направленных на дальнейшее проникновение в сеть. Это могут быть программы, распространяющиеся внутри сети, или команды другим скомпрометированным системам на атаку какого-либо узла.

- Сокрытие следов.

  Атакующий пытается удалить следы своего проникновения в сеть. Это могут быть изменения журналов, дат запуска файлов, сокрытие использованного программного обеспечения.

Для моделирования описанного поведения используется механизм тестов. Тест - это абстракция попытки атакующего использовать тот или иной способ взаимодействия с оборудованием. При этом тот вариант взаимодействия с оборудованием, который приведет к возможности эксплуатации вернет значение ИСТИНА, то есть злоумышленник добился цели на данном этапе.

При моделировании атак, так же необходимо учитывать уровень подготовленности атакующего и степень его мотивации. При использовании в качестве модели деревьев атак, подобные дополнительные факторы могут быть учтены в качестве исходных условий и вероятностью с которой при заданных условиях будет совершен рассматриваемый шаг. Для используемого метода моделирования, в котором не используются диаграммы атак, описанные условия будут влиять на процесс выбора атакующим того или иного способа взаимодействия(теста).

Список литературы

1. Realistic Modeling of Local Network Traffic Ph.D.Dissertation Proposal Stefan KarpinskiDepartme of Computer ScienceUniversity of California, Santa Barbara

2. Simulation of computer network attacks. Carlos Sarraute, Fernando Miranda, Jose I.Orlicki CoreLabs, Core Security Technologies ITBA(Instituto Technologico de Buenos Aires)

3. Modeling network attacks Major Scott D. Lathrop, Lieutenant Colonel John M.D.Hill, Lieutenant Colonel John R. Surdu Information Technology and operations Center. Department of Electrical Engineering and computer science United states military academy