Имитационные модели исследования характеристик систем защиты информации распределенной сети

Балами Исмайлов

Национальная Академия Авиации

balemi@rambler.ru

***Аннотация*— Разработаны имитационные модели систем защиты информации распределенных сетей с применением языка моделирования General Purpose Simulation System (GPSS). Приводятся результаты модели имитации системы защиты информации сети.**

Ключевые слова— распределенные сети; система защиты информации; модели имитации;

I. ВВЕДЕНИЕ

Известно что, проблема защиты информации в сети с каждым днем становится более значимой. Большинство негативных воздействий на распределенные сети (РС) осуществляется извне, в основном из глобальной сети INTERNET, превратившуюся в последнее время не только в средство поиска информации, но и в средство распространения вирусов, троянских коней и других вредоносных программ. Кроме того, защита информации в РС усложняется из-за различных причин, как большое число пользователей и их переменный состав. Анализ показывает, что защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц, а большое число потенциальных каналов проникновения в сеть еще усложняет защиту информации в сети.

Анализ показывает, что недостатки в аппаратном и программном обеспечении зачастую обнаруживаются в процессе эксплуатации сети и даже неидеальны современные встроенные средства защиты информации в таких известных и мощных сетевых ОС, как WINDOWS NT или NET WARE.

Порождаются новые проблемы связанные с защитой информации, когда осуществляется соединение с другими сетями и подключения к сети INTERNET и, следовательно, при этом увеличивается возможность поражения сети компьютерными вирусами [1].

Анализ показывает, что перечисление возможных угроз сети практически невыполнимо из за нескончаемого их количества. Поэтому на основе некоторых характерных особенностей таких как запрограммированные или незапрограммированные действия, засорение почтового ящика, нахождение черных ходов, загромождения канала, разрушения компьютера и т.д., проведены следующие основные классификации возможных угроз сети:

- Троянский конь представляет собой программу, работающую в фоновом режиме и представляющую полный доступ к данному компьютеру извне. Злоумышленник может воспользоваться ею для получения доступа к компьютерной сети, причем в этом случае его возможные действия ограничиваются лишь его фантазией (в отличие от запрограммированных действий вирусов);
- Вирусы могут распространяться даже в безобидных документах WORD и EXCEL. В отличие от троянских коней, вирусы выполняют лишь заранее запрограммированные действия;
- Сообщения, засоряющие почтовый ящик- это почтовые сообщения, направленные пользователем электронной почты, которые несут в себе рекламный контекст или просто бессмысленный текст. Посланные в огромном количестве они могут засорить почтовый ящик и не дать возможность получить нужную почту;
- Черные ходы представляют собой лазейки оставленные разработчиками программных продуктов и могут быть рассмотрены как разновидность троянских коней;
- Атаки, нацеленные на отказ сервиса, в основном применяются против серверов в сетях. Атаки представляют собой отказ определенного сервиса или всего сервера путем загромождения пропускного канала;
- Некорректно работающие программы могут быть использованы злоумышленниками в целях разрушения компьютерной сети.

В работе задача определения характеристик систем защиты информации (СЗИ) решается в рамках данной классификации возможных угроз сети т.е. учитываются характеристики воздействия возможных угроз на функционирование сети. Исходя из практических соображений число таких злоумышленных программ (заявок) составляет треть от общего числа заявок.

II. МОДЕЛЬ ИМИТАЦИИ СИСТЕМЫ ЗАЩИТЫ

Анализ показывает, что специализированные программные средства защиты информации от несанкционированного доступа обладают лучшими возможностями, чем встроенные средства сетевых ОС.

Известны программные средства обеспечения защиты информации, включая программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной информации типа временных файлов, тестового контроля системы защиты и др.

При решении проблемы связанной с защитой информации в РС предлагается решение задачи по определению оптимальной программно-технической структуры системы защиты информации, рассмотрением ее как многоканальной системы массового обслуживания (СМО). Рассмотренная СЗИ создается между РС и глобальной сетью, которые инспектируют и фильтруют проходящую через них информацию. Такая структура позволяет резко снизить угрозу несанкционированного доступа в РС извне, применяя при этом способ маскарада (masquerading), когда весь исходящий из РС трафик посылается от имени СЗИ делая РС практически невидимой. В таких сетях информация может передаться из различных источников синхронным и асинхронным образом [2].

С целью защиты информации в РС от внешних воздействий возникают задачи организации СЗИ имеющие современные программные технические структуры. СЗИ позволяет вести контроль над передачей информации и комплексную защиту информации от различных воздействий. СЗИ могут содержать следующий комплекс программ, который требует определенный объем памяти:

- Программы, осуществляющие криптографическое шифрование почтовых сообщений, таких как Pretty Good Privacy (PGP);
- Утилиты, позволяющие обнаруживать и уничтожать «шпионские» программы, например Ad-aware или X cleaner;
- Брандмауэры, обнаруживающие и блокирующие несанкционированный доступ к компьютеру, не допускающие попадания на жесткий диск «мусора», «шпионского» программного обеспечения и троянов;
- Антивирусные ПО (Antiviral Toolkit, Kaspresky antivirius, Dr.Web и др.) различные утилиты, направленные на борьбу с конкретными вирусами.

Следует отметить, что периодическое проведение анализа эффективности характеристики СЗИ является одной из основных задач РС. Совершенствование и оптимизация характеристик СЗИ позволяет разработать достаточно простую и эффективную СЗИ, которую трудно преодолеть даже опытному злоумышленнику.

ЗАКЛЮЧЕНИЕ

В заключении отметим, что предложенный подход основан на фундаментальных идеях теории системы и сетей, разработаны модели имитации исследования СЗИ как СМО с применением языка GPSS, и получены результаты, которые могут быть применены при построении РС различного назначения.

БИБЛИОГРАФИЯ

[1] В.А. Герасименко, А.А. Малюк, Основы защиты информации. М., Наука, 1997, 224 с.

[2] С.В. Алябов, "Проблемы защиты информации сети промышленного предприятия", Сб. трудов, выпуск 8, Воронеж, пуки, 2003, с.69.