ПРИМЕНЕНИЕ СЕТЕЙ ПЕТРИ В ОБУЧАЮЩЕЙ СИСТЕМЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

Калинина Н.А.
Сибирский государственный технологический университет
г. Красноярск, Россия

В связи с переходом организаций и предприятий на электронный документооборот постоянно повышается роль информационной безопасности в современном мире. Однако практическая подготовка инженеров-программистов оставляет желать лучшего, особенно в области сетевой безопасности. Причина заключается в том, что организация специальных сетей для учебных целей – весьма дорогостоящее мероприятие, и практическое обучение, как правило, проводится в обычных компьютерных классах. В этих условиях очень желательно наличие специальных обучающих систем, способных моделировать сетевые сегменты, атакующие воздействия и операции по формированию политики безопасности.

Актуальность создания обучающих систем по защите информации общепризнанна, и проводится работа по их созданию [1,2,3,4]. Однако большинство известных работ предлагают обучающие системы по теоретическому изучению защиты информации, практически современные интерактивные электронные учебники [1,2]. Другое направление исследований – создание обучающих аппаратных комплексов [3,4]. Это интересные и эффективные обучающие средства, однако заведомо дорогостоящие. Очень немногие разработки посвящены программным реализациям обучающих систем по приобретению практических навыков настройки и конфигурирования параметров сетевой безопасности.

В СибГТУ г.Красноярска создана программная обучающая система настройки политики сетевой безопасности, которая использует сети Петри для моделирования атакующих воздействий. Архитектура обучающей системы представлена на рис. 1. Система моделирует сегмент корпоративной сети, используя для этого схемы возможных сетевых топологий, перечень сетевых узлов (сетевых объектов), и перечень программного обеспечения (ПО), которое может быть установлено на каждом сетевом узле. При выборе устанавливаемого ПО можно определить тип операционной системы (ОС), количество разделов на жестком диске, тип файловой системы для каждого раздела, и перечень установленных прикладных программ. Кроме того, в качестве специальных защитных средств нужно определить права пользователей по отношению к каждому разделу жесткого диска и настройки межсетевого экрана на входе в сеть. Списку установленного программного обеспечения соответствует список его уязвимостей, созданный на основе международных публичных баз данных уязвимостей программного обеспечения, таких как CVE [6].

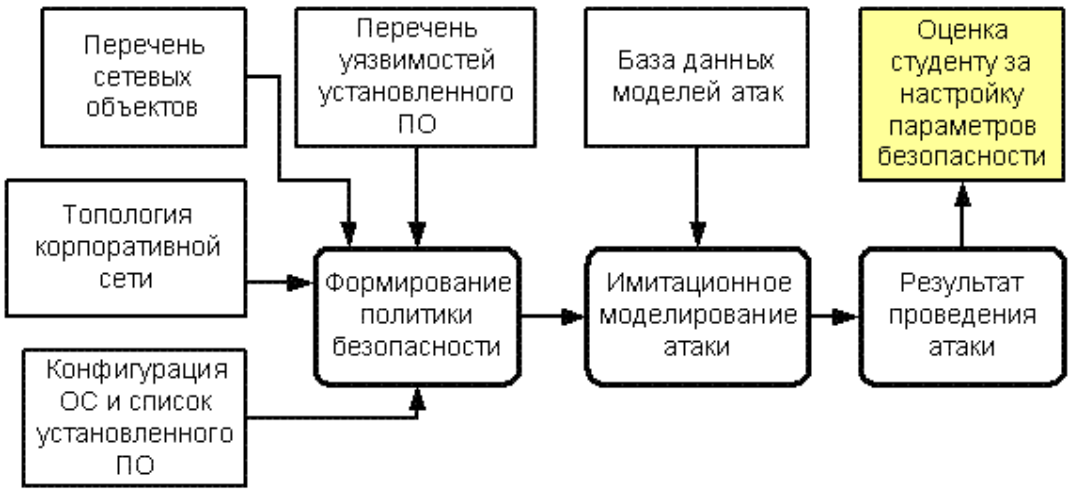

Рис.1 – Архитектура обучающей системы сетевой безопасности

Важной особенностью разработанной системы является учет уязвимостей ПО. Наличие уязвимости напрямую определяет возможность той или иной сетевой атаки, и представляется очень важным дать почувствовать студенту эту связь выбранного ПО и возможности реализации определенных видов атак. В общем случае ведение базы данных уязвимостей - весьма трудоемкая и дорогостоящая процедура, которая финансируется либо федеральными структурами развитых стран, либо крупными компаниями. Однако для учебных целей возможно ведение выборочной, неполной базы уязвимостей, что и сделано для созданной обучающей системы.

После выбора всех возможных настроек, влияющих на политику безопасности, проводится проверка ее адекватности путем имитационного моделирования атакующих воздействий на сетевые узлы. Моделирование осуществляется при помощи базы данных моделей атак, использующих сети Петри. Каждая возможная атака описывается следующими реквизитами:

- список портов (сетевых протоколов), которые должны быть открыты для реализации атаки
- степень опасности атаки для сетевого узла
- типовую вероятность выполнения атаки
- степень квалификации нападающего, необходимую для выполнения атаки
- перечень возможных результатов атаки
- краткое описание атаки
- сеть Петри, описывающую этапы проведения атаки и условия, необходимые для реализации каждого этапа

При моделировании атакующих воздействий анализируется квалификация нарушителя, предпринявшего атаку. В международной практике принято приблизительно оценивать квалификацию нарушителя, необходимую для реализации атаки. В базе данных моделей атак использованы оценки необходимой квалификации, взятые из базы данных CAPEC [5]. Если квалификация достаточна, далее проводится анализ всех условий, необходимых для проведения атаки. При анализе необходимых условий используется сеть Петри, моделирующая атаку. При отсутствии условий атака считается нереализованной. При наличии всех условий моделируется случайный процесс, с заданной для этой атаки вероятностью приводящий к ее реализации либо нереализации. Оценка правильности настроек определяется соотношением количества предпринятых и реализованных атак.

Библиографический список

1. Дьяченко Ю.А. Автоматизированная система дистанционного обучения и тестирования МИФИ «ИБ» [Электронный ресурс] / Режим доступа: *http://library.mephi.ru/data/scientific-sessions/2002/9_Konf/1155.html*
2. Райкин И.Л., Ляпина А.А. Автоматизированная обучающая система «Информационная безопасность и защита информации». – Труды Всероссийской конференции «Технологии Microsoft в теории и практике программирования» 19-20 марта 2008 г. Нижний Новгород, 2008.
3. Кистерева С.Н. Разработка и использование в учебном процессе виртуальных лабораторных комплексов при подготовке специалистов в области информационной безопасности // Молодёжь XXI века - будущее Российской науки": Материалы докладов IV Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных (12-14 мая 2006 г.). Выпуск V - Ставрополь
4. Дураковский А.П., Трегубов Д.Ю. Интерактивный лабораторный практикум по исследованию эффективности защиты средств вычислительной техники от утечки информации [Электронный ресурс] / Режим доступа: *http://library.mephi.ru/data/scientific-sessions/2008/z15/0-1-22.doc*
5. Common Attack Pattern Enumeration and Classification [Электронный ресурс] / Режим доступа : *http://capec.mitre.org/data/dictionary.html*
6. Common Vulnerabilities and Exposures [Электронный ресурс] / Режим доступа : *http://Cve.mitre.org*