

Говорят, что в КС реализовано иерархическое ролевое управление доступом *RBAC-H*, если любая субъект-сессия $s \in S$ пользователя $user(s) \in U$ может обладать правом доступа $p \in R_r$ к сущности $e \in E$ тогда и только тогда, когда истинен предикат $can_access(s, e, p)$.

Таким образом, модель *RBAC-H* ориентирована на КС, в которых уровень иерархии сущностей является существенным при определении политики управления доступом. Добавление атрибутов иерархии и типов сущностей к элементам моделей *RBAC* позволяет адаптировать последние к условиям функционирования реальных КС, а также существенно упростить реализацию и администрирование политики ролевого управления доступом.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology. Role Based Access Control (RBAC) and Role Based Security. [Электронный ресурс]. Режим доступа: <http://csrc.nist.gov/groups/SNS/rbac>.
2. Kuhn D. R., Coyne E. J., and Weil T. R. Adding attributes to role-based access control // IEEE Computer. 2010. No. 43(6). P. 79–81.
3. Sandhu R. S. and Mohammad A. A. A Model for Attribute-Based User-Role Assignment // Proc. 18th Annual Computer Security Applications Conf. San Diego, California, USA, December 09–13. IEEE Computer Society Washington, 2002. P. 353.
4. Десянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.

УДК 681.322

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ» НА ПЛАТФОРМЕ CISCO PACKET TRACER

Д. Н. Колегов, Б. Ш. Хасанов

Рассматриваются вопросы организации и проведения лабораторного практикума «Основы построения защищённых компьютерных сетей» на кафедре защиты информации и криптографии Национального исследовательского Томского государственного университета [1]. Практикум представляет собой набор лабораторных работ, которые могут использоваться в рамках одноимённого курса, курса «Вычислительные сети» или курсов смежной тематики. Актуальность данного практикума определяется тем фактом, что в настоящее время компьютерные сети являются ключевой составляющей современных информационно-телекоммуникационных систем. Среди всех задач по построению компьютерных сетей важнейшей является обеспечение защищённости от угроз конфиденциальности, целостности и доступности. При этом подсистема защиты должна являться частью компьютерной сети, обеспечивающей её безопасность, как одно из возможных свойств. При таком подходе к разработке архитектуры компьютерных сетей говорят о защищённых компьютерных сетях.

Целью лабораторного практикума является получение знаний, необходимых при проведении работ по проектированию защищённых компьютерных сетей, а также навыков настройки механизмов безопасности и средств функционирования сетевой инфраструктуры.

Задачей лабораторного практикума является получение знаний и навыков по следующим направлениям:

- архитектуре и методам проектирования защищённых компьютерных сетей;
- планированию и построению подсистем защиты информационных технологий;
- настройке механизмов и средств защиты сетевой инфраструктуры;
- поиску и устранению неисправностей в системах защиты компьютерных сетей.

В настоящее время лабораторный практикум включает следующие работы:

1. Защита инфраструктуры маршрутизации на базе протоколов OSPF, EIGRP и BGP.
2. Защита инфраструктуры коммутации.
3. Построение отказоустойчивой локальной вычислительной сети (ЛВС) на базе протокола STP.
4. Защита ЛВС от атак канального уровня.
5. Построение маршрутизируемой ЛВС с высокой доступностью.
6. Защита сетевой инфраструктуры от несанкционированного доступа.
7. Настройка механизмов качества обслуживания в сети передачи данных.
8. Защита передачи голосовых данных в IP-сети.
9. Защита периметра сети.
10. Криптографическая защита каналов передачи данных от несанкционированного доступа.
11. Защита беспроводной ЛВС.

Для обеспечения лабораторных работ используется программный эмулятор сетей «Cisco Packet Tracer». Данное программное обеспечение позволяет:

- проводить одновременно лабораторный практикум для группы обучающихся численностью до 25 человек;
- эмулировать и изучать все основные процессы функционирования реальных компьютерных сетей;
- моделировать некоторые атаки в компьютерных сетях (например, VLAN hopping, MAC-spoofing, атаки на протокол STP);
- предоставить в распоряжение обучающегося виртуальную компьютерную сеть, при этом отсутствует необходимость создания дорогостоящих учебных стендов реального сетевого оборудования.

По усмотрению преподавателя, дополнительно к указанным лабораторным работам в рамках практикума может проводиться :

1. Многопользовательская игра между группами обучающихся в режиме реального времени по методологии [2].
2. Решение задачи «Поиск и устранение неисправностей в компьютерной сети». Преподавателем подготавливается конфигурационный файл модели компьютерной сети, часть которой настроена и функционирует некорректно. Обучающиеся имеют доступ к части сетевого оборудования. Задача обучающихся найти и устранить ошибки в настройке сетевого оборудования и средств защиты в заданное время.
3. Ролевая игра «Разработка защищённой корпоративной сети передачи данных». Перед обучающимися ставится задача построения двух корпоративных сетей передачи данных в соответствии с выданным техническим заданием на проектирование и политикой безопасности. Обучающиеся делятся на две группы. Каждый студент назначается ответственным за проектирование и настройку

отдельного модуля сети (например, периметр Интернет, ЦОД, ЛВС, сеть филиала). Затем все сегменты соединяются через сетевые механизмы Cisco Packet Tracer. После развёртывания сетей обучающиеся меняются сетями и модулями. При этом решаются задачи изучения и анализа конфигурации новой сети, поиска и устранения ошибок проектирования и реализации, если таковые имеются. На протяжении всей игры преподавателем могут даваться различные вводные инструкции по изменению политик безопасности, порядка функционирования сетевой инфраструктуры и требований к сетям передачи данных.

ЛИТЕРАТУРА

1. Колегов Д. Н. Обучение на платформе CISCO основам построения защищённых вычислительных сетей // Прикладная дискретная математика. Приложение. 2010. № 3. Р. 53–55.
2. Morozov E. Cisco Packet Tracer King-of-the-Hill Multiuser Game [Электронный ресурс]. Режим доступа: http://www.netskills.hu/regisztracio/sites/upload/conf2011/prezi/1-8_evgeny_morozov.pdf

УДК 004.94

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ МАНДАТНОГО И РОЛЕВОГО УПРАВЛЕНИЯ В СИСТЕМЕ *RSBAC*

П. Ю. Свиридов

Рассматриваются особенности реализации мандатных и ролевых механизмов системы управления доступом *RSBAC* [1] в операционной системе (ОС) GNU/Linux. Система *RSBAC* разработана в 1996–1997 гг. Амоном Оттом в целях повышения безопасности ОС на базе ядра Linux и представляет собой надстройку над ядром и набор утилит администрирования. Система построена в соответствии с архитектурой *GFAC*, предложенной Абрамсом и ЛаПадула, и состоит из нескольких модулей безопасности, каждый из которых реализует определенную политику безопасности.

В системе *RSBAC* реализованы механизмы безопасности, использующие следующие политики управления доступом:

- RC (*Role Compatibility*) — политика совместимости ролей Отта;
- MAC (*Mandatory Access Control*) — мандатная политика Белла — ЛаПадулы;
- ACL (*Access Control Lists*) — дискреционная политика на основе механизма списков доступа;
- PM (*Privacy Model*) — политика защиты персональных данных на основе модели Фишер-Хабнера;
- FF (*File Flags*) — политика назначения флагов доступа файлам;
- Auth (*Authenticated User*) — политика авторизации пользователей.

Основными особенностями реализации механизмов управления доступом в системе *RSBAC* являются:

- ассоциирование с каждой сущностью ОС множества атрибутов, отражающих их различные свойства, необходимые для реализации политик управления доступом (например, атрибутами субъектов ОС являются их роли и уровни доступа в рамках ролевой и мандатной модели управления доступом соответственно);
- использование более 30 различных видов доступа и прав доступа;
- использование многоуровневой решетки безопасности;