Лабораторная работа №1

Управление доступом с помощью списков контроля доступа.

Часть 2.
Управление доступом к приложениям и системам базам данных

Теоретические основы

Многие приложения предоставляют возможность со стороны сервера настраивать те или иные параметры, влияющие на безопасность системы. Активируя те или иные параметры, администратор системы может повышать или понижать общую безопасность системы.

В большинстве случаев повышение безопасности системы увеличивает неудобства для пользователей, уменьшает возможности системы и усложняет реализацию тех или иных функций системы.

Пользователь программного продукта должен работать с минимально возможным уровнем привилегий. Нарушение этого правила может привести к таким ситуациям как:

- предоставление атакующему возможности нанесения вреда в большей мере в случае непредвиденной ситуации;
- непреднамеренное нарушение защищённости информации со стороны пользователя.

В определённый момент жизненного цикла программы может произойти сбой: в таком случае атакующий может воспользоваться нештатной ситуацией и обеспечить себя привилегиями, которые назначены уязвимому процессу, уязвимой пользовательской учётной записи и т. д.

Например, в случае, если процесс работает с правами администратора или суперпользователя, или максимальные привилегии предоставлены учётной записи пользователя, вредоносный код, в случае возникновения непредвиденной ситуации, может также быть выполнен с правами администратора, суперпользователя или максимальными привилегиями в системе.

Также в результате атаки, пользователю может быть предоставлен доступ к данным, которые в обычной ситуации для него недоступны. Это может быть в том случае, когда данные доступны для атакованной подсистемы, которая обладает достаточными привилегиями для обращения к данным.

Существует большое количество систем, которые имеют сложную организацию

механизма контроля доступа к объектам системы: механизм контроля доступа к объектам файловой и операционной систем, механизм контроля доступа непосредственно в системе (например веб-приложению), механизм контроля доступа к различным подсистемам (например к системам управления базами данных).

Инструментальные и вспомогательные средства

1. Виртуальная машина с установленной ОС (Windows, Linux).

Задание для самостоятельной работы

1. Создать программу, которая позволяет установить веб-приложение или систему управления базами (СУБД) данных в зависимости от выбранного варианта.
2. Создать программу, которая позволяет настроить механизм контроля доступа для выбранного веб-приложения или СУБД.
3. Создать программу для проверки корректности работы настроенной политики безопасности выбранной СУБД или веб-приложения.
4. Создать программу, которая позволяет удалить веб-приложение или СУБД, а также созданные ими объекты файловой системы, в зависимости от выбранного варианта
5. Оформить отчёт о проделанной работе.

Политика безопасности выбранного веб-приложения или СУБД должна быть настроена следующим образом. В системе должны присутствовать следующие роли:

- администратор системы с полным доступом ко всем подсистемам веб-приложения и с максимальными привилегиями,
- пользователь с полными либо частичными правами в подсистеме, предоставленной администратором,
- гость с правами только на чтение отдельных фрагментов, предоставленных администратором.

Варианты веб-приложений и СУБД

- Jenkins – веб-приложение для управления и контроля таких задач, как непрерывная интеграция, управление жизненным циклом приложений, управление

удалёнными системами и т. д.

- Redmine – веб-приложение для управления проектами и задачами ,
- OpenFire – веб-приложение, позволяющее клиентам в режиме реального времени обмениваться сообщениями,
- SVN сервер – веб-приложение, которое предоставляет возможность централизованного управления системой контроля версий,
- Git сервер – веб-приложение, которое предоставляет возможность централизованного управления распределённой системой контроля версий,
- Apache Tomcat – веб-приложение, которое предоставляет возможность работы в режиме сервера приложений,
- WildFly – веб-приложение, которое предоставляет возможность работы в режиме сервера приложений,
- MySQL (MariaDB) – реляционная СУБД,
- Mongo – документно-ориентированная СУБД,
- PostgreSQL – реляционная СУБД;
- другое веб-приложение или СУБД.

Отчётность

В качестве результата ожидается:

1. Демонстрация работы программ, которые позволяют обновить систему безопасности выбранного приложения или СУБД.
2. Демонстрация работы настроенного веб-приложения или СУБД.
3. Демонстрация работы программы для проверки корректности работы разработанной политики безопасности.
4. Отчёт о проделанной работе.

Отчёт должен быть оформлен в соответствии с http://www.bsuir.by/m/12_100229_1_80040.pdf.

Отчёт должен содержать следующую информацию.

1. Постановка задачи.
2. Краткое описание выбранного веб-приложения или СУБД.
3. Описание созданных программ для обновления политики безопасности выбранного веб-приложения или базы данных.
4. Вывод. В выводе должны быть представлена семантическая и прагматическая составляющие проделанной работы.

Список рекомендуемых источников

1. Официальный сайт CWE: Common Weakness Enumeration [Электронный ресурс]. - Электронные данные. - Режим доступа: http://cwe.mitre.org/ Дата доступа: 20.08.2014. ID: 250, 264-280.
2. Ховард, М. Защищённый код // М. Ховард, Д. Лебланк — М.: Русская редакция, 2004. — 704 с., главы 6, 7.
3. Ховард, М. 24 смертных греха компьютерной безопасности. Библиотека программиста // М. Ховард, Д. Лебланк, Дж. Вьега — СПБ.: Питер, 2010. — 400 с., главы 12, 16, 17 (с. 211-225, 262-283).
4. Низамутдинов, М. Ф., Тактика защиты и нападения на Web-приложения // М.Ф. Низамутдинов. — Спб.: БХВ-Петербург, 2005. 432 с.
5. Официальный сайт Jenkins [Электронный ресурс]. - Электронные данные. - Режим доступа: http://jenkins-ci.org/ Дата доступа: 20.08.2014.
6. Официальный сайт Redmine [Электронный ресурс]. - Электронные данные. - Режим доступа: http://www.redmine.org/ Дата доступа: 20.08.2014.
7. Официальный сайт OpenFire [Электронный ресурс]. - Электронные данные. - Режим доступа: http://www.igniterealtime.org/projects/openfire/ Дата доступа: 20.08.2014.
8. Официальный сайт Git [Электронный ресурс]. - Электронные данные. - Режим доступа: http://git-scm.com/ Дата доступа: 20.08.2014.
9. Официальный сайт WildFly [Электронный ресурс]. - Электронные данные. - Режим доступа: http://wildfly.org/ Дата доступа: 20.08.2014.
10. Официальный сайт MySQL [Электронный ресурс]. - Электронные данные. - Режим доступа: http://www.mysql.com/ Дата доступа: 20.08.2014.
11. Официальный сайт MongoDB [Электронный ресурс]. - Электронные данные. - Режим доступа: http://www.mongodb.org/ Дата доступа: 20.08.2014.
12. Официальный сайт PostgreSQL [Электронный ресурс]. - Электронные данные. - Режим доступа: http://www.postgresql.org/ Дата доступа: 20.08.2014.