Лабораторная работа №2

Анализ защищённости приложений

Часть 1.
Оценка защищённости разработанного приложения

Теоретические основы

Одним из важнейших аспектов разработки практически любой системы является защита конфиденциальной информации. В качестве конфиденциальной информации могут выступать идентификационные, персональные данные пользователей, конфигурационные данные различных систем и многие другие.

Среди атак на программное обеспечение можно выделить:

- атаки на хранимые данные,
- атаки на канал передачи данных,
- социальная инженерия и другие типы несанкционированного доступа к программному обеспечению.

Наиболее популярными методами программных атак на сегодняшний день являются:

- полный перебор (или метод «грубой силы»),
- перебор по словарю,
- анализ трафика (например, с помощью сниффера),
- атака человек посередине,
- инъекция (SQL инъекция, PHP инъекция, скрипт-инъекция или XSS, XPath инъекция и другие),
- использование уязвимостей в коде,
- DoS (Denial of Service – отказ в обслуживании) и DDoS (Distributed Denial of Service) атаки,
- удалённое управление доступом,
- специальные программы (вирус, руткит, троянский конь и т. д.) и другие.

Существует ряд мер, позволяющих повысить уровень защищённости конфиденциальной информации программного обеспечения. Среди таких мер можно выделить:

- анализ кода на безопасность,
- физическая безопасность устройств, на которые установлено программное обеспечение
- настроенная политика безопасности в операционной системе,
- настроенная сетевая политика безопасности,
- настроенная политика безопасности каждого компонента программного обеспечения и каналов взаимодействия между ними,
- организационные меры защиты,
- юридические меры защиты.

Инструментальные и вспомогательные средства

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

Задание для самостоятельной работы

1. Разработать приложение, которое позволяет
   - добавить пользователя в систему,
   - авторизовать пользователя на основе идентификационных данных,
   - создать, редактировать, удалить, осуществить поиск конфиденциальных данных,
   - создать, редактировать, удалить, осуществить поиск неконфиденциальных данных,
   - деавторизовать авторизованного пользователя.
2. Выполнить анализ разработанного приложения с точки зрения
   - политики безопасности операционной системы,
   - политики безопасности компонентов приложения и их взаимодействия между собой,
   - сетевой политики безопасности,
   - безопасности конфиденциальности данных.
3. Оформить отчёт о проделанной работе.

Отчётность

Результат выполненной работы должен быть представлен в виде
- демонстрации работы созданного приложения,
- демонстрации защищённости разработанного приложения,
- обоснования защищённости разработанного приложения,
- отчёта 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 разработанного приложения.
3. Анализ защищённости приложения.
4. Анализ защищённости конфиденциальной информации.
5. Вывод. В выводе должны быть представлена семантическая и прагматическая составляющие проделанной работы.

Список рекомендуемых источников

1. Ховард, М. Защищённый код // М. Ховард, Д. Лебланк — М.: Русская редакция, 2004. — 704 с.
2. Ховард, М. 24 смертных греха компьютерной безопасности. Библиотека программиста // М. Ховард, Д. Лебланк, Дж. Вьега — СПБ.: Питер, 2010. — 400 с.
3. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. - СПб.: БХВ-Петербург, 2009. - 576 с.