Digital Security

Особенности проведения тестов на проникновение в организациях банковской сферы

Илья Медведовский, к.т.н.

Директор Digital Security

Тест на проникновение систем ДБО

Тест на проникновение систем ДБО – два вектора:

- Клиентская часть ПО
  - Безопасность ActiveX
  - Безопасность работы ПО с ЭЦП
- Серверная часть системы
  - Серверное ПО системы ДБО
  - ПО обслуживающих серверов (ОС, СУБД, Веб-сервер)

Безопасность клиентской части Интернет-Банка

С точки зрения злоумышленника, пользователь Интернет-Банка является более простой и удобной целью атаки, чем сам банк:

- Пользователь защищен слабее банка
- Пользователей гораздо больше – выше шансы

Результат атаки: получение доступа к любым операциям со счетами клиента и ключам ЭЦП.

Но:

- **ответственность клиента**
- **ущерб репутации банка**

Безопасность серверной части Интернет-Банка

Внешний нарушитель

- Атакует внешний периметр и программное обеспечение Интернет-Банка

Внешний нарушитель – пользователь интернет-банка

- Имеет счет (привилегированный пользователь)
- Атакует приложение, используя свою учётную запись

Результат атаки: компрометация базы данных, получение доступа к банковской тайне, компрометация клиентов, получение доступа ко всем счетам, отказ в обслуживании

Типовые уязвимости Банк-Клиентов

Уязвимости клиентской части

- Использование уязвимостей **сервера**, направленных на клиента (например, уязвимости WEB: CSRF, XSS)
- Использование уязвимостей браузера
- Использование уязвимостей компонентов браузера
- Фишинг

Уязвимости серверной части

- Уязвимости WEB (SQL Injection, Local File Including, Code Execution, etc)
- Использование уязвимостей программного обеспечения сервисов, например, веб-сервера.

Пример проникновения

При проведении теста на проникновение были обнаружены две уязвимости в системе ДБО:

- уязвимость типа XSS на странице аутентификации банк-клиента
- уязвимость переполнения буфера в клиентском компоненте ActiveX ДБО

Используя обе уязвимости, был создан демо-эксплойт, который выполняет произвольный код и внедряет его в URL с помощью уязвимости XSS. Таким образом мы получаем сценарий атаки на клиентов банка, использующий уязвимости как на стороне банка (XSS), так и на стороне клиента (выполнение кода), и позволяющий получить неавторизованный доступ к рабочей станции, которая работает с банк-клиентом.

Опыт компании по анализу защищенности Банк-Клиентов

- Специализация по поиску уязвимостей в Банк–Клиентах: публикация информации о найденных уязвимостях на закрытом банковском форуме АРЧЕ.
- Проведение анализа защищенности систем Интернет-Банка основных российских разработчиков: BSS, INIST, R-Style InterBank.

  Результат работ показал, что большая часть систем ДБО содержит уязвимости, позволяющие нанести ущерб. За 2009 год было найдено множество уязвимостей, среди которых:
  - Buffer Overflow - выполнение произвольного кода
  - Ошибки в реализации - обход аутентификации
  - SQL Injection - доступ к БД
  - XSS - фишинг, атака на клиентов

Особенности теста на проникновение в соответствии с PCI DSS

- Требование 11.3 стандарта PCI DSS
- Область применения – область обработки, хранения, передачи карточных данных (рабочие станции, серверы, сетевое оборудование) – **то есть все объекты, попадающие под QSA-аудит**
- Один раз в год или после серьезных изменений инфраструктуры
- Цель – **проникновение (а не доступ к данным!)**

Методика проведения тестов на проникновение

Тест на проникновение

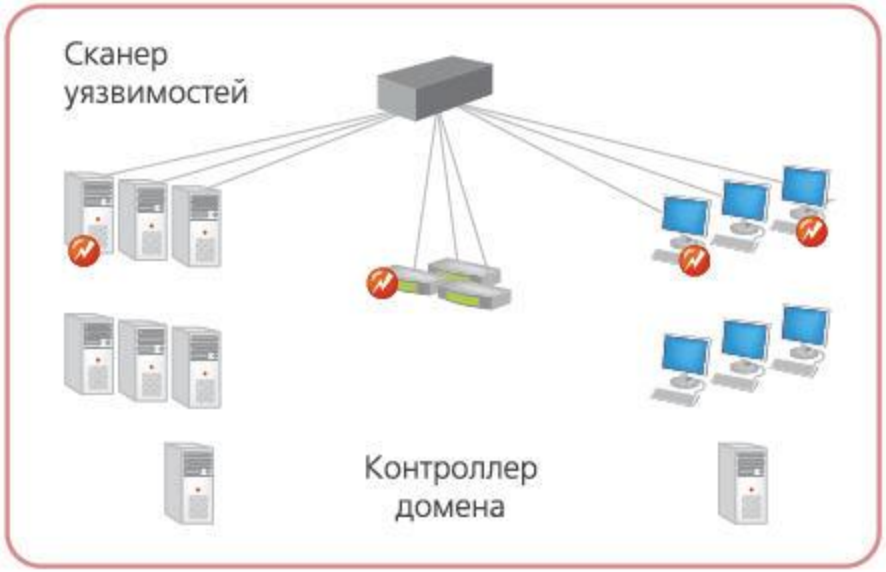
- Внешний периметр (из сети Интернет)
- Внутренний периметр (внутри корпоративной сети)

Алгоритм проникновения

- Поиск уязвимостей
- Реализация уязвимостей
- **Продвижение вглубь системы**
- Обход существующих систем защиты

Алгоритм сканера

- Поиск уязвимостей по сигнатурам
- Генерация отчёта


Сканер
уязвимостей
Контроллер
домена


Активный
аудит
Контроллер
домена

Задача – проникновение (не сканирование!)

Проникновение – получение доступа к ИС

- Карточные данные – не цель; **цель – среда.**
- Если есть доступ к среде, значит карточные данные не защищены.

! Шифрование данных не является достаточной защитой:

- возможность получения доступа к данным до или после проведения криптографических процедур;
- перехват аутентификационных данных.

Итоговый вывод об успешном прохождении теста на проникновение в данном случае делает только QSA-аудитор

Качество теста на проникновение

Качество теста на проникновение

- Опыт
- Исследования в области ИБ
- Квалифицированные специалисты

Контроль Совета PCI SSC

К критичным нарушениям QSA-аудитором процедуры проверки относятся:

- Заведомо ложная трактовка аудитором требований стандарта
- Обозначение в Отчете о Соответствии невыполненного требования как выполненного
- Тест на проникновение – не просто сканирование
- Отзыв статуса QSA у аудитора – проблемы с сертификатом у его заказчика

Пример внутреннего теста на проникновение

- Была подобрана учетная запись(DBSNMP) по умолчанию к тестовому серверу СУБД ORACLE.
- Данный сервер оказался связан БД-линком с основным сервером БД под непривилегированной учётной записью.
- Используя данный линк, была найдена уязвимость SQL-инъекции в хранимой процедуре основного сервера БД. Используя эту уязвимость, удалось повысить свои права до администратора БД.

Опыт компании

- С 2002 года основные направления деятельности компании: проведение активного аудита защищенности внутренней сети, анализ защищенности бизнес-приложений, систем ДБО и тесты на проникновение. С 2008 года компания обладает статусом QSA и имеет ряд успешно завершенных проектов по сертификации на соответствие PCI DSS.
- Созданный в 2007 году международно признанный исследовательский центр по поиску и анализу уязвимостей – **DSecRG**. Исследовательский центр имеет множество официальных благодарностей от таких компаний как: SAP, Oracle, IBM, HP.
- В 2009 году Digital Security совместно с АРЧЕ создали открытое сообщество профессионалов **PCIDSS.RU** и выступают организаторами международной конференции **PCI DSS Russia**

Спасибо за внимание!