Digital Security

Тест на проникновение в соответствии с PCI DSS

Илья Медведовский
Digital Security
Директор, к.т.н.

Кто? Что? Зачем?

- 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**.

© 2002—2009, Digital Security

Что это?

Тест на проникновение

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

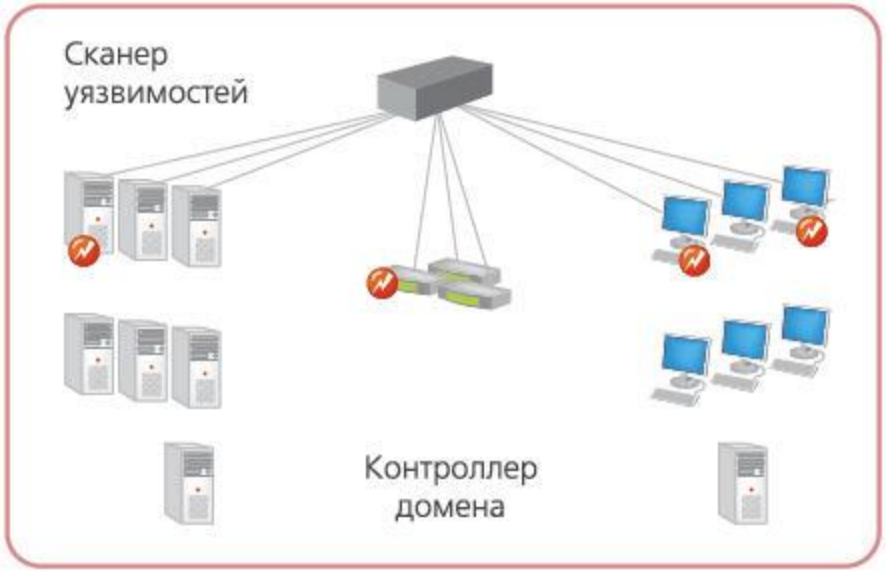
Алгоритм проникновения

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

Алгоритм сканера

- Поиск уязвимостей по сигнатурам.
- Генерирования отчёта.

© 2002—2009, Digital Security


Сканер
уязвимостей
Контроллер
домена

Активный
аудит
Контроллер
домена

Что показывает?

Объективная реальность

- Эффективность систем защиты.
- Адекватность конфигурации ОС серверов и рабочих станций, баз данных и активного сетевого оборудования.
- Эффективность СУИБ в целом:
  - управление обновлениями;
  - парольная политика;
  - система журналирования и оповещения.
  - информированность пользователей

© 2002—2009, Digital Security

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 пентеста делает только QSA-аудитор

© 2002—2009, Digital Security

Качество теста на проникновение

Качество теста.

- 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

© 2002—2009, Digital Security

Пример внутреннего теста на проникновение

- Найдена уязвимость хранимого межсайтового скриптинга на внутреннем портале.
- Внедряется код, который перенаправляет в невидимом фрейме браузер пользователя на ресурс созданный специалистом проводящим тест на проникновение..
- Проведение атаки SMB RELAY для аутентификации на контроллере домена используя NTLM пользователя.
- Используя аутентификацию пользователя, специалист пробует выполнить код на контроллере домена – запуск командной строки.
- Когда администратор посетил портал, на контроллере домена откроется черный ход – командная строка с правами доменного администратора.

© 2002—2009, Digital Security

Пример внутреннего теста на проникновение

Итог

- Получен доступ с правами администратора к контроллеру домена.

Ошибки

- Уязвимость типа XSS.

ВОПРОСЫ

www.dsec.ru

www.dsecrg.ru

www.pcidss.ru

© 2002—2009, Digital Security