Летняя сессия Уральского форума
«Информационная безопасность финансовой сферы»
PCI DSS Russia 2017

Лучшие практики
проведения обязательных тестов на проникновение для подтверждения статуса PCI DSS

Москва, 31.05.2017

…Обо мне…

Алексей Плешков

Образование

- окончил МИФИ в 2006 году факультет «Информационная безопасность»
- специалист по информационной безопасности банковских систем

Опыт работы

- более 16 лет в сфере ИБ,
- 12 лет в банке ТОП-3 РФ,
- эксплуатации средств защиты,
- проведение проверок и прохождение аудитов,
- выявление внутренних и внешних нарушителей, противодействие высоко технологическому мошенничеству, киберразведка, аналитическая работа,

О pen-test PCI DSS

Цель: получение практического подтверждения эффективности системы защиты данных платежных карт

Основание: требование п. 11.3 стандарта PCI DSS v. 3.2

Объект аудита (scope): места обработки (в т.ч. хранения, изменения, тиражирование, передачи и пр.) данных платежных карт (PAN, cardholder name, CVV2…)

Периодичность: min раз в 0,5 года
(либо после любых (v.3.2) изменений в инфраструктуре объекта аудита)

Места обработки данных

Инфраструктура процессингового центра
Инфраструктура финансовой организации
Клиентская часть ПО ДБО

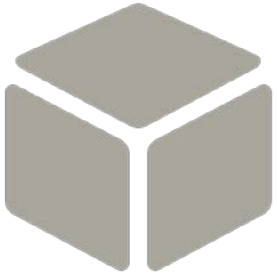
- толстый клиент (мобильное приложение)
- тонкий клиент (JavaScript, ActiveX)

Серверная часть ПО ДБО:

- фронтальное решение (ОС, Web-сервер, СУБД)
- сопутствующие сервера (МСЭ, E-mail и пр.)

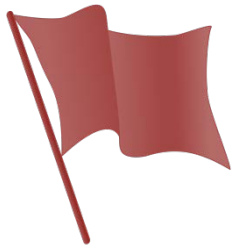
Торгово-сервисные предприятия
Сеть терминалов (банкоматы, POS, кассы)

Pen-test методики

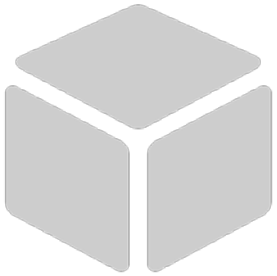


GrayBox

интерактив с атакуемым



Red Team



WhiteBox

максимум результата

BlackBox

реальная жизнь

Blue Team

Модель нарушителя

- Внешний хакер без доступа к ПО ДБО
- Клиент с доступом в ДБО
- Внешний хакер без доступа к инфраструктуре
- Сотрудник процессингового центра
- Работник сервисной организации

Вектора pen-test для PCI DSS

- Поиск уязвимостей в ДБО (п. 11.3.2)
- Подготовка и реализация демо-эксплоитов (п. 11.3.2)
- Сканирование Wi-Fi сетей на объекте (п 11.1.b)
- Сканирование внешнего периметра сети организации из Интернет (п. 11.2, 11.3.1)
- Поиск уязвимостей в системе удаленного доступа (пп. 2.3.b, 3.6.5.a, 8.1.5.a, 8.3, 12.3)

- Социальная инженерия в отношении работников (пп. 8.2.2.,11.4.b)
- Поиск и мотивация бывших сотрудников (п. 11.4.b)
- Работа с сервисными организациями и партнерами (пп. 8.5.1, 11.3.4.b)

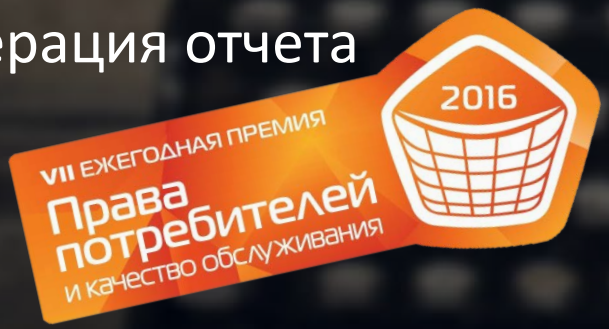
Чего «НЕ делают» в рамках pen-test

- Получение прямого доступа к реальным данным платежных карт
- Нарушение доступности основных сервисов
- Привлечение излишнего внимания
- Кибербразведка / Darknet
- Черный рынок
- Шантаж/подкуп должностных лиц
- Консультирование/обучение работников

Сценарии pen-test

Простой (внешний сканер)

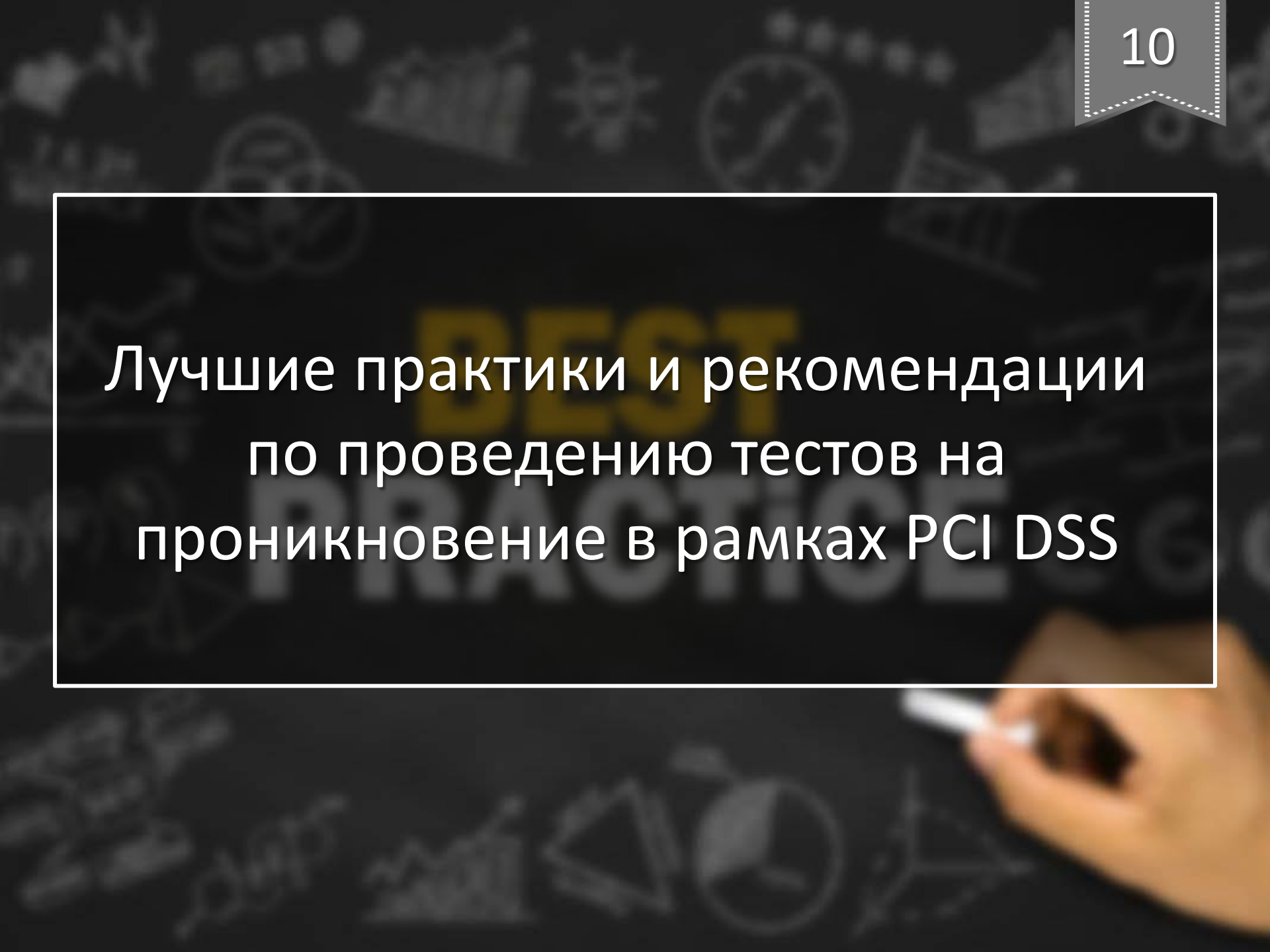
- Согласование scope
- Удаленный умный поиск уязвимостей (признаков отсутствия обновлений) по справочникам сигнатур
- Генерация отчета



Проникновение

- Внешнее сканирование
- Экспертная диагностика
- Реализация уязвимостей
- Закрепление
- Поиск уязвимостей в доступном контуре
- Продвижение вглубь защищенного периметра
- Согласование результатов
- Подготовка отчета

Лучшие практики и рекомендации по проведению тестов на проникновение в рамках PCI DSS



Best practice # 1

Проведите pen-test собственными силами

Best practice # 2

Применяйте практику red team / blue team

Best practice # 3

Приглашайте различных QSA-аудиторов

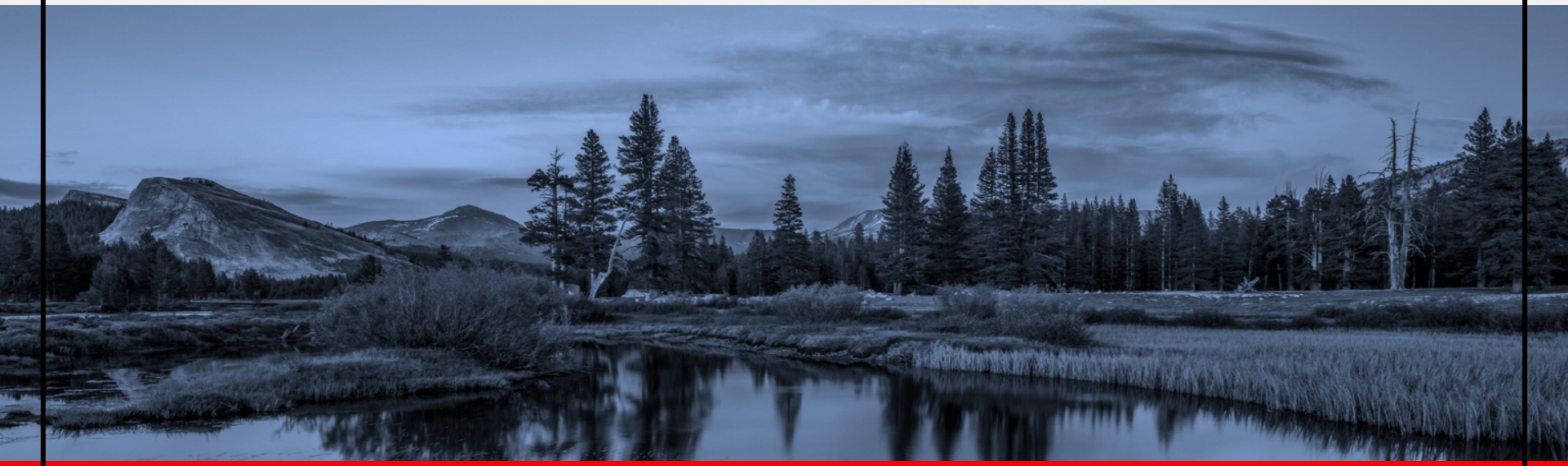
Best practice # 4

Включите журналирование всех событий

Best practice # 5

Регулярно проводите «разбор полетов»

Благодарю за внимание!



Готов ответить на Ваши вопросы