Сыграем в игру …
Подход QIWI к проведению тестирования на проникновение

Ермаков Кирилл,
директор по информационной безопасности Группы QIWI

О себе

- Кирилл Ермаков, CTO/CISO Группы QIWI
- Эксперт по безопасности WEB-приложений
- Также известен под псевдонимом ‘isox’
- Участник “Зала славы” Yandex, Mail.ru, Apple и других компаний

Тестирование на проникновение или «анализ защищенности»

- Способ проверки контролей ИБ
- Fast and dirty assessment («Быстрый способ оценки защищенности»)
- Выполняется квалифицированными специалистами
- Обязательная/рекомендованная часть регламентирующих документов:
  - ✓ ФЗ-152 (пункт 8.8)
  - ✓ СТО БР ИБСС-1.0-2014 (пункт 7.3.1)
  - ✓ Положение 382-П (пункты 2.5.1, 2.5.3)
  - ✓ PCIDSS (пункты 11.2 и 11.3)
- Независимая оценка защищенности компании от угроз ИБ

Классический подход

- Выделенная команда (2-5 человек)
- Сценарии: внешний нарушитель, внутренний нарушитель, социальная инженерия методом рассылки писем
- Множество запрещенных техник и подходов (DOS, кража техники и т.д.)
- «Белый список» адресов атакующих в системах ИБ
- Отсутствие информации об устройстве компании «изнутри»
- Запрет на полноценную «социальную инженерию»
- Атаки производятся в рабочее время

Взгляд со стороны специалиста

- Подход не меняется в зависимости от заказчика
- По ⅓ времени
  - эксплуатация известных векторов атак
  - поиск новых уязвимостей
  - сканирование автоматическими средствами
- Запрет на нарушение физических границ предприятия
- Ограниченные возможности по получению данных нетехническими способами
- «Поставленный на поток» процесс

Red Team Exercise: учения по противодействию угрозам ИБ

- Зарубежное название данного подхода – Red Team Exercise
- Подразделение ИБ не оповещается о проводимых учениях
- Попытка симулировать «настоящую атаку»
- Выполняется одной командой «атакующих»
- «Внутренняя кухня» компании по-прежнему не разглашается

Недостатки данного подхода

- «Слепые зоны»
- Ограничения по времени
- Не используются многие сценарии, применяющиеся в реальных атаках
- Слишком этичный и аккуратный подход
- Реальный злоумышленник атакует по другому
- Недостаточные ресурсы одиночной команды

Нарушим классические подходы

- Объединим лучших профессионалов в «сборную»
- Не будем придерживаться «методологий проведения тестирований на проникновение»
- Никаких «секретных технологий взлома»
- Снимаем ограничения по времени проведения атак
- Для атак доступны любые системы
- Никакой подготовки со стороны подразделения ИБ

Разрешим «запретный плод»

- Любые нетехнические способы получения информации
- Вредоносное программное обеспечение
- Перебор паролей учетных записей
- Атаки по ночам и в выходные дни
- Физическое проникновение на территорию компании
- Атаки, направленные на отказ в обслуживании
- Несанкционированные подключения в сеть предприятия
- Кража персонального оборудования сотрудников
- «Подкуп» специалистов компании

Добавим «крота»

- Сотрудник компании, играющий за команду атакующих
- Разглашает приватную информацию
- Обладает компетенцией по системам ИБ и особенностям их работы
- Предоставляет карту сети
- Дает советы и подсказки

Глубокий анализ защищенности

- Проверка контролей физической безопасности
- Манипуляции с сетью предприятия:
  - ✓ Врезка в кабель
  - ✓ Атаки на беспроводные сети
  - ✓ Подброшенные USB-накопители с вредоносным ПО
- «Социальная инженерия» в реальной жизни
- Использование информации с «украденных» ноутбуков, телефонов, планшетов

Проверка работоспособности отдела ИБ

- Оценка скорости реакции сотрудников, ответственных за информационную безопасность
- Анализ настоящих инцидентов ИБ
- Проблемы отработавших защитных механизмов (блокировки и недоступность учетных записей)
- Подстройка систем ИБ «на лету»
- Взаимодействие с подразделениями, ответственными за физическую безопасность
- Анализ журналов, записей камер видеонаблюдения, событий ИБ

Условия победы

- Для команды атакующих:
  - ✓ Получение доступа к учетной записи администратора приложений или баз данных
  - ✓ Захват контроллера домена компании
  - ✓ Компрометация учетной записи администратора *nix систем
  - ✓ Несанкционированный доступ к любой критичной системе
- Для отдела ИБ предприятия:
  - ✓ Обеспечение безопасности активов компании

Тестирование на проникновение: подход QIWI

- Команда атакующих: Digital Security и ONSEC
- Команда защиты: отдел ИБ группы компаний QIWI
- «Крот»: Руководитель подразделения ИБ
- Продолжительности атаки: 2,5 месяца
- Цель атакующих:
  - Компрометация чувствительной информации
- Цель обороняющихся:
  - Зарегистрировать в системе мониторинга инцидентов ИБ не менее 90% действий нарушителей
  - Не допустить получения доступа к системам компании

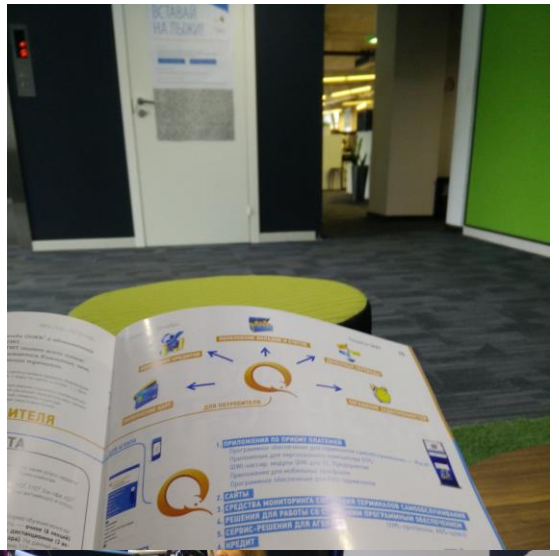
Недели «осады»

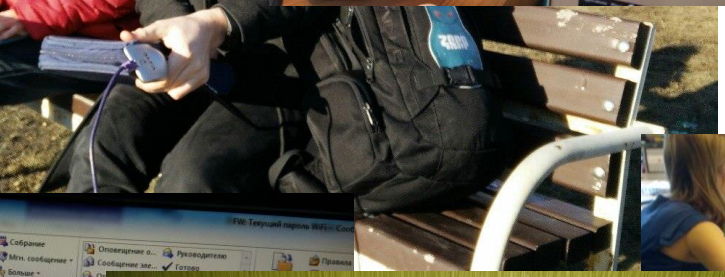
- 7 социальных атак за 2 недели
- Несколько «критичных» инцидентов
- Вывод из строя ПО компании (отказ в обслуживании)
- Серьезные нарушения работоспособности предприятия:
  - ✓ Заблокированные учетные записи
  - ✓ Рассылки вредоносных писем
  - ✓ Заражения вредоносным ПО
- Вынужденное проведение анализа вредоносного кода

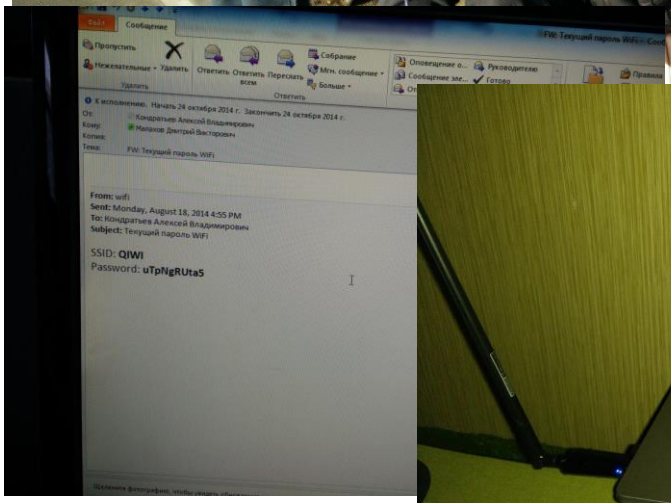
Найдены серьезные уязвимости

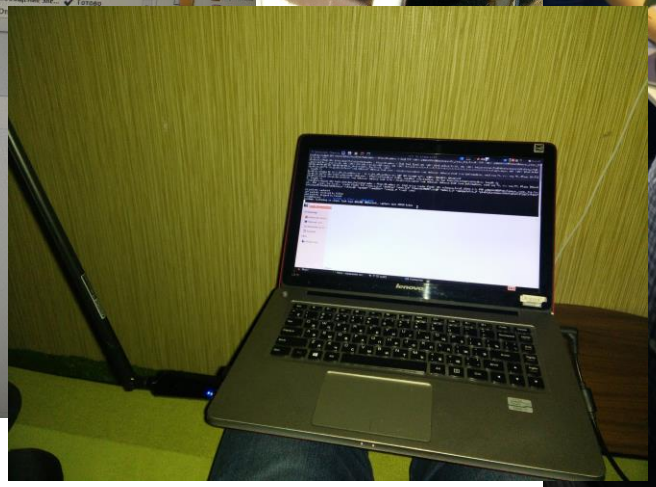
- Удачное проникновение злоумышленников в здание компании
- Компрометация сети предприятия через взлом компьютеров, находящихся в гостевой беспроводной сети
- Множественные уязвимости реализации подключения ПО Apple MacOS к контроллеру домена Microsoft
- Взлом «умного дома»
- Захват системы управления источником бесперебойного питания
- Компиляция утилиты dsniff для операционной системы системы видеонаблюдения

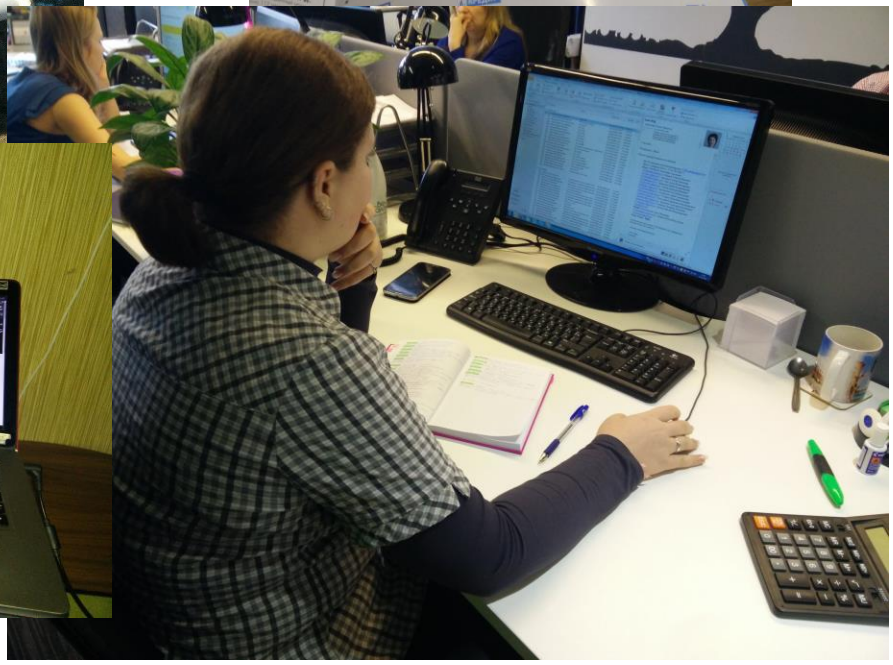
Несколько фотографий процесса











Результат: команда «защиты» проиграла

- Учетная запись с повышенными привилегиями была скомпрометирована
- «Социальная инженерия» – лучший вектор для атаки
- Был получен удаленный SSH-доступ к ноутбуку сотрудника информационной безопасности
- Несанкционированный доступ к архиву конфигураций сетевого оборудования
- Множественные удачные атаки методом перебора

Удачный сценарий атаки

- Получение пароля учетной записи методом социальной инженерии
- Эксплуатация отсутствия изоляции в гостевой беспроводной сети
- Ноутбуки, подключенные одновременно к проводной и беспроводной сети
- Ошибка конфигурирования подключения Apple MacOS к домену Microsoft, разрешавшая подключение любого существующего пользователя к любому ПК
- Хранение чувствительной информации без ограничения на ее просмотр на жестком диске ПК
- Недостаточный контроль каналов передачи данных в офисной сети

Анализ результатов проведенной работы

- Данный подход эффективнее классического
- Атака была близка к методам, используемым реальными злоумышленниками
- Прекрасное покрытие ресурсов компании
- Оценка реальной защищенности, а не того, как ее показывают руководители ИБ
- Вы разочаруетесь в эффективности ваших технических средств противодействия угрозам ИБ
- Данный подход дороже классических
- Необходимо быть готовым к непредсказуемым последствиям (недоступность систем)

Благодарности

Команде ИБ Группы QIWI за терпение

Специалистам Digital Security и ONSEC

за прекрасную работу

Благодарности

Вопросы?

isox@qiwi.com