Заказной тест на проникновение: инструмент ИБ или…

Василий Томилин,
ведущий специалист

vtomilin@cisco.com

Тест на проникновение

- Имитация действий реального злоумышленника
- Цель: выявление существующих уязвимостей и, возможно, практическое их использование в демонстрационных целях.

Результат

- Отчет (описание уязвимостей, способов их использования и способов устранения обнаруженных уязвимостей)
- Что дальше?

Тест на проникновение: особенности

- Работа весьма квалифицированных специалистов
- Существенно превосходит простой запуск сканеров уязвимостей
- Слабо формализуемые процедуры (методологии описывают общие подходы, конкретика определяется особенностями тестируемой системы и выбором экспертов-аудиторов)

Результат для заказчика

- Тест на проникновение прошел успешно
- Было обнаружено 15 уязвимостей
- Они делятся по уровням (приложения, инфраструктура)
- Они делятся по категориям риска (критично, важно, средне, малоопасно)
- Их можно устранить указанными в отчете способами

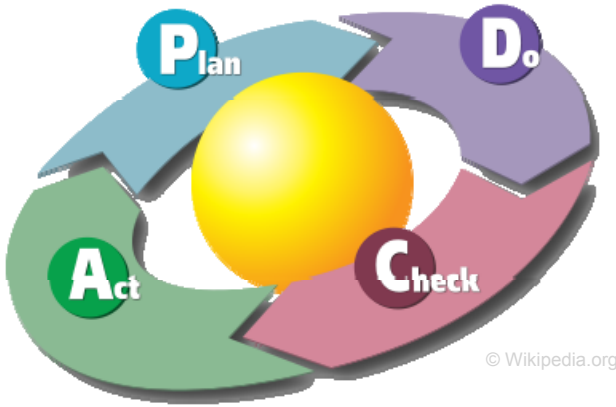
Вопросы

Насколько повысилась защищенность системы?

Какова полнота тестирования?

Модель PDCA

- Plan. Определение конечных целей, разработка плана действий
- Do. Реализация плана действий
- Check. Проверка созданной реализации
- Act. Анализ результатов проверки. Достигнуты ли цели? Не обновились ли цели? Необходимо ли повторить цикл?
- При следовании комплексному подходу к обеспечению информационной безопасности тест на проникновение входит в этап C, являясь методом проверки (аудита)



© Wikipedia.org

Тест на проникновение – метод проверки (аудита)

- Проверка подразумевает:
  - формализацию области проведения проверки;
  - формализацию критериев определения результата проверки;
  - сужение возможных методик проверки.
- Кто должен это делать?
  - компания, проводящая тест на проникновение? Владеет ли эта компания всей нужной информацией, особенно при проведении black box/Black hat теста?
  - заказчик или подрядчик + заказчик? Всякий ли заказчик может поставить задачу, ответ на которую принесет ему пользу?
- Проблема «зрелости» заказчика

Тест на проникновение: весь этап аудита или только часть?

- Нужен ли для решения этих задач тест на проникновение?
  - В конфигурации сетевого устройства допущены ошибки Как их эффективнее найти: получить санкционированный доступ к конфигурации и проверить ее или получить НСД через Интернет?
  - Как эффективнее обнаружить некорректность состояния вычислительной системы: проверить по Security Configuration чек-листу или провести атаку с использованием нестандартного эксплойта?
- Польза для заказчика
  - Что полезнее для заказчика: факт взлома сервера из-за неустановленного патча или неверной настройки или набор рекомендаций по корректной настройке сервера?

Тест на проникновение: условия применимости в качестве средства аудита

- Существование объекта аудита (*зрелость заказчика*)
  - Наличие этапа P (проработанные политики безопасности, формализованные критерии безопасности и т. п.)
  - Наличие этапа D (реализованная архитектура системы обеспечения безопасности, работоспособные средства обеспечения безопасности, продуманные процессы обеспечения безопасности)
- В противном случае: тест по Шнайеру

Тест на проникновение или «типовой» аудит

Критерий	Тест на проникновение	«Типовой» аудит
Квалификация исполнителей	Сверхвысокая	В соответствии с ИТ-инфраструктурой
Время обнаружения очевидных проблем внутренней ИТ-инфраструктуры	Меньшая оперативность (дополнительные затраты времени на проникновение)	Максимальная оперативность
Полнота охвата	Фрагментарная (если восстанавливается полная ИТ-инфраструктура, потрачено лишнее время)	Полная
Возможность оценки изначального состояния защищенности	Отсутствует	Присутствует
Возможность оценки конечного состояния защищенности	Отсутствует	Присутствует
Предсказуемость результата	Отсутствует	Присутствует
Уровень	Практический	Более теоретический
Поддержание уровня ИБ	Метод «проб и ошибок»	Системный подход
WOW-эффект	Высокий	Низкий

Инструмент обеспечения ИБ/ повышения уровня защищенности

Критерии

- Возможность оценки изначального состояния защищенности
- Возможность оценки конечного состояния защищенности
- Формализуемая оценка полноты охвата

Тест на проникновение едва ли соответствует этим характеристикам

Тест на проникновение: зачем?

- Наглядная демонстрация
- Практическая проверка теоретических предпосылок (дополнение к «типовому» аудиту)
- Независимый аудит фактического положения дел (контроль качества)

Тесты на проникновение являются превосходным и эффективным дополнением типового аудита.

Тест на проникновение: ключевой вопрос экспертов самим себе

- Будет ли тест на проникновение шагом аудита системы обеспечения информационной безопасности или просто наглядной демонстрацией очевидного?

  или

- Готов ли заказчик к проведению теста на проникновение?

  или

- Надо ли стрелять из пушки по воробьям?

Тест на проникновение: побочные причины проведения

- Источник прибыли (относительно *рутинная* задача повышения защищенности превращается в экспертную *уникальную* услугу)
- Элемент конкурентной борьбы (несостоятельность другого решения)
- Повышение внимания к вопросам ИБ (и нуждам подразделения/специалистов по ИБ)
- Дополнительная реклама компании и подтверждение квалификации экспертов-аудиторов
- Привлекательность услуги вследствие ее «романтического флера»

Выводы

- При следовании системному подходу тесты на проникновение абсолютно применимы в качестве одного из этапов аудита информационной безопасности
- Критерием применимости тестов на проникновение является текущее состояние процессов обеспечения информационной безопасности у заказчика
- Автономный тест на проникновение позволяет устранить ряд уязвимостей на несистемной основе
- Автономный тест на проникновение не вполне корректно позиционировать как инструмент обеспечения ИБ или инструмент повышения уровня защищенности