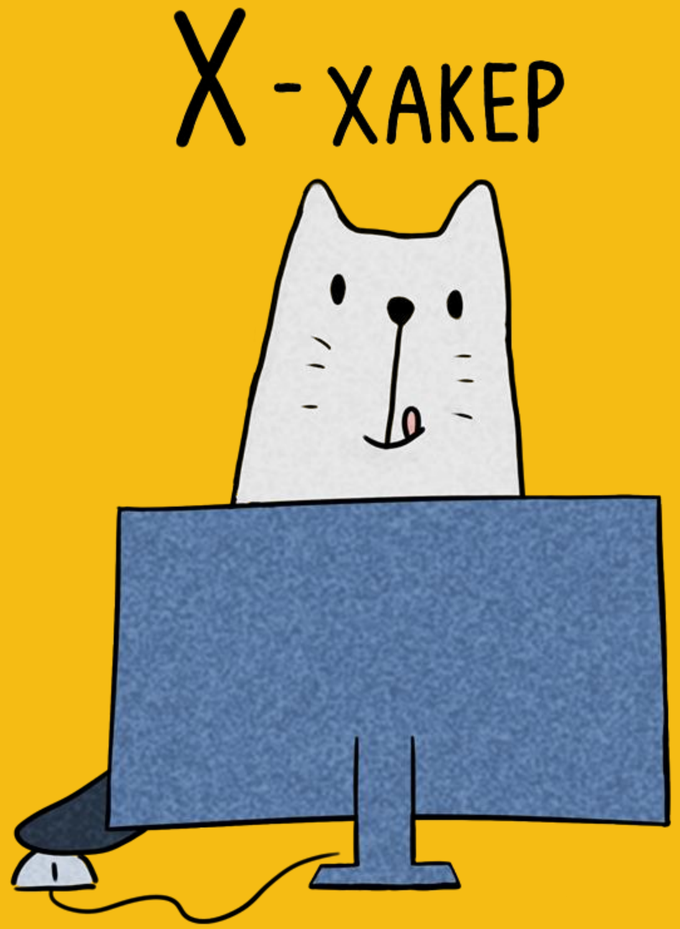
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК ПЕРЕЖИТЬ ПЕНТЕСТ?

Как организовать и провести тестирование на проникновение и ничего не сломать



Швецов Константин
Ведущий эксперт Регионального Центра Развития «Казань» Центрального Банка РФ

PENETRATION TEST VS VULNERABILITY ASSESSMENT

Тестирование на проникновение ставит своей основной задачей именно проникновение в систему, получение доступа к закрытой информации и «заметание следов».

Аудит (или оценка) уязвимостей проводится с целью нахождения максимального числа уязвимостей в заданной области и подразумевает проникновение и получение привилегий в системе.

КОМУ НУЖЕН PENTEST?

Регулятивные требования:

382-П п. 2.5.5.1 - Оператору по переводу денежных средств, оператору услуг платежной инфраструктуры на стадиях создания и эксплуатации объектов информационной инфраструктуры необходимо обеспечить: ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

PCI DSS 3.2 п. 11.3 - Внедрить методологию проведения тестирования на проникновение
п. 11.3.1 - Проводить внешний тест на проникновение не реже одного раза в год
п. 11.3.2 - Выполнять внутренний тест на проникновение не реже одного раза в год

Приказ ФСТЭК №239 п. 12.6 При проведении анализа уязвимостей применяются следующие способы их выявления: д) тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

КОМУ ЕЩЁ НУЖЕН PENTEST?

«Стресс-тестирование» вашей системы информационной безопасности.

Внутреннее соответствие политике информационной безопасности организации.

Следование лучшим практикам безопасной разработки ПО

Стандарты и фреймворки

PTES
Penetration Test Execution Standard разработан группой практических экспертов по информационной безопасности из разных отраслей

OWASP Testing Framework
Разработан и поддерживается участниками Open Web Application Security Project

OSSTMM
Open Source Security Testing Methodology Manual разработан Институтом Безопасности и Открытых Методологий (ISECOM)

CHECK framework
Разработан Национальным Центром Кибербезопасности (часть Британского Центра правительственной связи)

NIST SP 800-115
Разработан Национальным Институтом Стандартов и Технологий США

ЭТАПЫ ПЕНТЕСТА

1 ПЛАНИРОВАНИЕ

2 РАЗВЕДКА

3 СКАНИРОВАНИЕ

4 ЭКСПЛУАТАЦИЯ (ПОЛУЧЕНИЕ ДОСТУПА)

5 ПОСТ-ЭКСПЛУАТАЦИЯ (ЗАКРЕПЛЕНИЕ В СИСТЕМЕ)

6 СОКРЫТИЕ СЛЕДОВ

7 АНАЛИЗ

8 ОТЧЁТ

ЧЕМ БОЛЬШЕ ВНИМАНИЯ УДЕЛЕНО ПЕРВОМУ ЭТАПУ

— тем меньше боли на остальных и выше ценность результата.

#CODEIB

ПЛАНИРОВАНИЕ ТЕСТИРОВАНИЯ

Определите целевую аудиторию тестирования

Какие системы или сервисы будут задействованы?
Кого из сотрудников и владельцев систем необходимо оповещать о тестировании?

Кто со стороны безопасности будет задействован?
Необходимо ли отработать штатный режим реагирования на инциденты?

Оповестите владельцев организации
Крайне желательно включать высший менеджмент в целевую аудиторию.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПЛАНИРОВАНИЕ ТЕСТИРОВАНИЯ

Определите требования для тестирования

Конфиденциальность полученных данных
Определите, кто должен быть немедленно оповещён, в случае нахождения критичных проблем

Действия на случай непредвиденных обстоятельств
Если в результате тестирования будут найдены следы прошедшего или текущего взлома злоумышленниками?

ПЛАНИРОВАНИЕ ТЕСТИРОВАНИЯ

Определите технические ограничения

Legacy системы
Определите хрупкие старые системы, которые остаются бизнес-критичными

Системы на внешних площадках
Какие проблемы могут возникнуть у хостинг-провайдеров?

Георасределенные системы
Как тестировать системы или их часть, которые расположены за границей основного периметра?

БЮДЖЕТ

— это основная движущая сила тестирования. Бюджет во многом определяет область и глубину тестирования, выбор средств и подходов.

Определите область тестирования

Тщательно продуманная и описанная область тестирования – залог более ценного отчёта по итогу

- Чётко определите, что вы хотите видеть в качестве конечного результата
- Определитесь со стратегией
  - Black box
  - Gray box
  - White box
- Обозначьте типы злоумышленников, действия которых вы хотите сымитировать
- Зафиксируйте модель угроз
- Обозначьте цели атак и определите их критичность для бизнеса
- Удостоверьтесь, что ваши средства обеспечения безопасности работают, согласно ваших требований
- Создайте и следуйте конкретному расписанию
- Найдите пути, как обезопасить себя от внезапного расширения области тестирования
- Опишите все необходимые выходные данные, включая протоколы встреч и совещаний

ПЛАНИРОВАНИЕ ТЕСТИРОВАНИЯ

Соглашение о проведении тестирования

Коммуникации
Чётко определена вертикаль коммуникаций с обоих сторон, так же как и лидеры проекта

Определены случаи и каналы немедленного оповещения
Случаи возможной деградации или остановки сервиса, следы текущих или прошедших взломов.

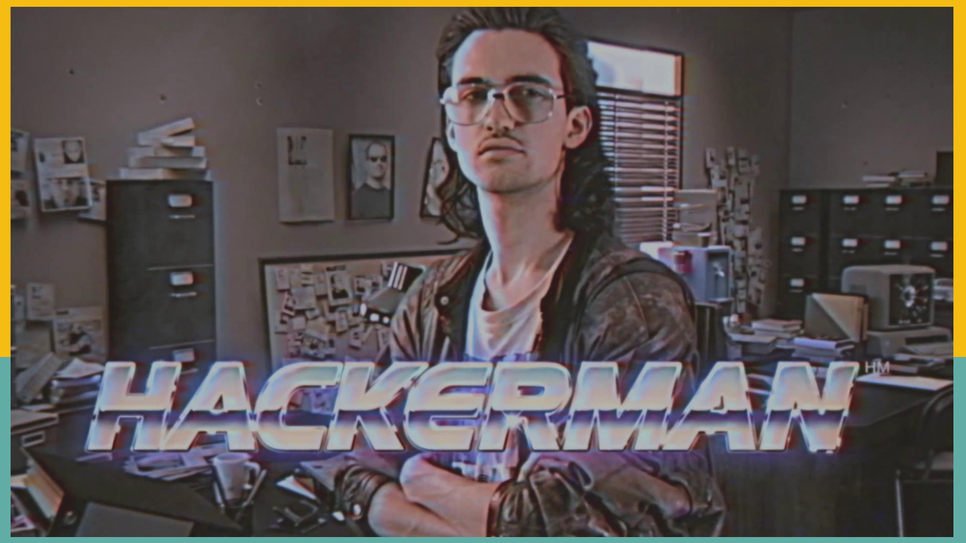
Намечены пути эскалации
В случае расширения области тестирования или появления проблем, не связанных с самим тестированием

Вы готовы к тестированию, если:

1. **Вы понимаете цель проведения пентеста**
2. **Чётко определён круг заинтересованных лиц, включая владельцев компании**
3. **Зафиксирован план действий, в случае непредвиденных обстоятельств**
4. **Определены и согласованы технические ограничения**
5. **Сформирован бюджет**
6. **Соглашение о тестировании содержит данные для коммуникаций с обеих сторон**

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ



shvetsovka@cbr.ru
+7 927 243 41 60

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ