Deloitte.

Тест сетей и систем на устойчивость ко взлому (pentest), или тест на проникновение

Что это?

Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) – это услуга в сфере информационной безопасности, суть которой заключается в санкционированной попытке проникнуть в информационную систему и обойти существующий комплекс средств ее защиты.

Процесс тестирования на проникновение предусматривает моделирование реальных действий злоумышленника, поиск уязвимостей системы защиты и их дальнейшую эксплуатацию. Тест на проникновение позволяет получить независимую оценку и экспертное заключение о состоянии защищенности конфиденциальной информации.

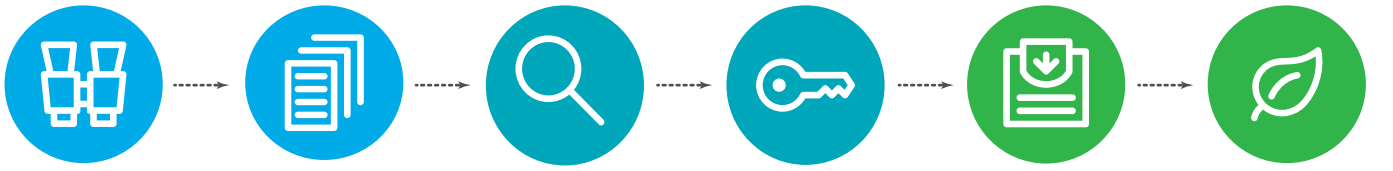
Зачем это нужно?

Разработанная компанией «Делойт» методология тестирования на проникновение поможет вам избежать инцидентов, которые могут подорвать репутацию вашей организации и нанести вам существенный ущерб.

Удачная реализация попытки эксплуатации обнаруженных уязвимостей ИС позволит продемонстрировать возможные пути проникновения в информационные системы (ИС), а также выявить слабые места в обеспечении информационной безопасности. Это позволит отделить критические проблемы безопасности, требующие пристального внимания, от тех, которые представляют меньшую угрозу.
А значит, появится возможность разумно выделять финансовые и материальные ресурсы на обеспечение безопасности ИС именно на тех участках, на которых это необходимо больше всего.

Как осуществляется (этапы)?

Методология компании «Делойт» по проведению тестирования на проникновение содержит **следующие этапы:**



Планирование теста на проникновение

Сбор публично доступных данных о целевых системах

Поиск уязвимостей ИС (сканирование)

Проникновение в систему (эксплуатация уязвимостей)

Написание и предоставление отчета

Очистка системы от последствий теста

1. Планирование теста на проникновение

На этом этапе определяются сроки, стоимость работ, которые будут проводиться, методы, которые будут применены, тип и количество ИС для тестирования и форма отчета.

Существует 3 подхода к проведению теста на проникновение:

White box
Исполнитель имеет доступ к системам и обладает полной информацией о них.

Grey box
Исполнитель имитирует хакеров, располагающих информацией об ИС частично (например, о диапазоне IP-адресов, web-сайтах, физическом расположении, идентификаторах беспроводных сетей и т. д.).

Black box
Исполнитель имитирует хакеров, которым известны только название компании и практически нулевые сведения о целевой системе.

2. Сбор публично доступных данных о целевых системах

В объем работ, как правило, входит **поиск информации из таких источников:**

- поисковые системы;
- социальные сети и сайты знакомств;
- каталоги предприятий;
- новостные сайты;
- корпоративные сайты компании-заказчика, сайты клиентов и партнеров;
- сайты поиска работы;
- базы данных WHOIS;
- DNS-серверы компании;
- анализ маршрутов сетевого оборудования;
- анализ e-mail писем;
- звонки в call-центр компании с целью получить информацию о ключевых сотрудниках компании, о структуре компании и технологии;
- анализ метаинформации в документах, размещенных на сайтах компании;
- непосредственное сканирование сети различными инструментами для выявления IP-адресов, портов, версий функционирующих сервисов и операционных систем.

Часто уже на этом этапе возможно выявление критических уязвимостей, таких как забытые или «бесхозные» сервисы, не требующие авторизации и дающие доступ к внутренней сети, опубликованные конфиденциальные данные, пароли и другая критическая информация.

3. Поиск уязвимостей ИС (сканирование)

В зависимости от выбранных систем на этом этапе сканируются уязвимости различными программами-сканерами. Специализация таких сканеров может быть ориентирована на тестирование периметра сети, web-сайтов, отдельных программ и сервисов: баз данных, VPN-устройств, устройств IP-телефонии и т. д.

4. Проникновение в систему (эксплуатация уязвимостей)

Найденные потенциальные уязвимости должны быть проверены вручную, чтобы отфильтровать все ложные срабатывания.

Этот этап предусматривает:

- верификацию и исследование уязвимостей;
- проведение атак на компоненты ИТ-инфраструктуры;
- подбор паролей;
- определение способов взаимодействия приложений;
- подтверждение выявленных уязвимостей;
- сбор доказательств.

Для взлома уязвимых ИТ-систем используются разный специализированный инструментарий, эксплойты в публичном доступе на хакерских сайтах. В некоторых случаях понадобится собственная разработка вирусов и эксплойтов для проникновения внутрь сети.

5. Написание и предоставление отчета

После проведения теста на проникновение разрабатывается отчет о тестировании, который обычно содержит:

- описание границ, в рамках которых был проведен тест на проникновение;
- методы и средства, которые использовались во время проведения теста на проникновение;
- описание выявленных дефектов и недостатков, в частности, уровня их риска и возможности их использования злоумышленником;
- описание примененных сценариев проникновения;
- описание достигнутых результатов;
- базовую оценку рисков информационной безопасности Компании;
- базовую оценку процессов обеспечения информационной безопасности Компании;
- рекомендации по устранению выявленных недостатков и совершенствованию процессов обеспечения информационной безопасности Компании;
- план работ по устранению найденных уязвимостей и совершенствованию процессов обеспечения информационной безопасности Компании, приоритезированный в соответствии с критичностью уязвимостей.

Результат (что получит заказчик)?

Основным преимуществом проведения теста на проникновение является усиление защищенности ИС, а именно:

- выявление максимального количества уязвимостей;
- принятие мер на основе обоснованных рекомендаций;
- уверенность в защищенности информации;
- выполнение требований контролирующих органов/стандартов;
- обоснование бюджетов подразделения на устранение упущений.

Продолжительность проведения теста на проникновение варьируется в зависимости от масштаба работы и уровня защищенности объектов тестирования.
Минимальный срок – от 2 недель.

Почему «Делойт»?

Команда «Делойт» – это сертифицированные специалисты в области тестирования на проникновение (CEH).

Мы обладаем знаниями лучших практик (Cobit), стандартов информационной безопасности (ISO/IEC 27001, ISO/IEC 27002, NIST800-115) и широким практическим опытом внедрения. Также наша команда обладает рядом техник для выявления уязвимостей целевой ИС, проникновения в ИС без ущерба бизнес-процессу компании и четкого описания реального состояния защищенности ИС.

Методика компании «Делойт» по проведению теста на проникновение разработана на основе общепризнанных международных методологий (PTES, PCI DSS, ISSAF).

deloitte.by

О «Делойт»