**Тестирование безопасности**

Это тип тестирования ПО, который выявляет уязвимости, угрозы и риски. Целью тестов безопасности является выявление всех возможных лазеек и слабых мест в ПО, которые могут привести к потере информации, доходов, репутации компании, сотрудников или клиентов. Общая стратегия безопасности основывается на трех основных принципах:

* Конфиденциальность - сокрытие определенных ресурсов или информации
* Целостность – ресурс может быть изменен только в соответствии с полномочиями пользователя
* Доступность - ресурсы должны быть доступны только авторизованному пользователю, внутреннему объекту или устройству

Тестирование безопасности обычно выполняет отдельный специалист по безопасности. В ходе тестирования безопасности испытатель играет роль взломщика. Ему разрешено все:

* попытки узнать пароль с помощью внешних средств;
* атака системы с помощью специальных утилит, анализирующих защиты;
* подавление, ошеломление системы (в надежде, что она откажется обслуживать других клиентов);
* целенаправленное введение ошибок в надежде проникнуть в систему в ходе восстановления;
* просмотр несекретных данных в надежде найти ключ для входа в систему.

При неограниченном времени и ресурсах хорошее тестирование безопасности взломает любую систему. Задача проектировщика системы — сделать цену проникновения более высокой, чем цена получаемой в результате информации.

Типы тестирования безопасности:

* Сканирование уязвимостей/оценка защищенности (Vulnerability Scanning) выполняется с помощью автоматизированного ПО для сканирования системы на наличие известных сигнатур уязвимостей.
* Сканирование безопасности (Security Scanning) включает в себя выявление слабых сторон сети и системы, а затем предоставляет решения для снижения этих рисков. Это сканирование может быть выполнено как ручным, так и автоматизированным.
* Тестирование на проникновение (Penetration testing) - этот тип тестирования имитирует атаку злоумышленника. Это тестирование включает анализ конкретной системы для проверки потенциальных уязвимостей при попытке внешнего взлома.
* Оценка рисков (Risk Assessment) тестирование включает анализ рисков безопасности, наблюдаемых в организации. Риски классифицируются как Низкие, Средние и Высокие. Это тестирование рекомендует меры по снижению риска.
* Аудит безопасности (Security Auditing) - внутренняя проверка приложений и операционных систем на наличие уязвимостей. Аудит также может быть выполнен путем построчной проверки кода
* Этический взлом (Ethical hacking) - совершается с целью выявления проблем безопасности в системе. Это делается White Hat хакерами - это специалисты по безопасности, которые использует свои навыки законным способом для помощи в выявлении дефектов системы, в отличии от Black Hat (преступников) или Gray Hat (что-то между).
* Оценка состояния (Posture Assessment) объединяет сканирование безопасности, этический взлом и оценки рисков, чтобы показать общее состояние безопасности организации.

|  |  |
| --- | --- |
| SDLC фаза | Security Processes |
| Requirements | Анализ безопасности для требований и проверка случаев злоупотребления / неправильного использования |
| Design | Анализ рисков безопасности для проектирования. Разработка плана тестирования с учетом тестирования безопасности |
| Coding and Unit testing | Статическое и динамическое тестирование безопасности и тестирование белого ящика |
| Integration testing | Тестирование черного ящика |
| System testing | Тестирование черного ящика и сканирование уязвимостей |
| Implementation | Тестирование на проникновение, сканирование уязвимостей |
| Support | Анализ воздействия патчей |

Доп. материал: