Вернуться назад

Что такое тестирование на проникновение?

16 марта, 2018 Евгений Архаров 0 Комментариев

Тестирование на проникновение является одной из методик выявления областей системы, уязвимых для вторжения и компрометации целостности и достоверности со стороны неавторизованных и злонамеренных пользователей или сущностей. Процесс тестирования проникновения включает в себя умышленные санкционированные атаки на систему, способные выявить как ее наиболее слабые области, так и пробелы в защите от сторонних проникновений, и тем самым улучшить атрибуты безопасности.

Данная методика также может быть использована в качестве дополнения к другим методам проверки для оценки эффективности комплекса защиты системы от различных типов неожиданных вредоносных атак.

Каковы причины уязвимостей системы?

Пробелы в безопасности появляются на разных стадиях процесса и зависят от множества факторов:

- ошибка проектирования (например, недоработки в дизайне – один из наиболее важных факторов возникновения лазеек в безопасности);
- некорректная настройка и неудачная конфигурация связанного оборудования и программного обеспечения;
- проблемы сетевого подключения (безопасное подключение устраняет возможность вредоносных атак, а небезопасная сеть обеспечивает шлюз хакерам для нападения на систему);
- человеческая ошибка (ошибка, совершенная преднамеренно или непреднамеренно отдельным лицом или командой при проектировании, развертывании и обслуживании системы или сети);
- погрешность коммуникации (неправильная или открытая передача конфиденциальных данных и информации среди команд или отдельных лиц);
- чрезмерная сложность системы (контролировать механизм безопасности простой сетевой инфраструктуры легко, а отслеживать утечки или любую злонамеренную деятельность в сложных системах трудно);
- недостаточность обучения (отсутствие знаний и должной подготовки по вопросам безопасности как у внутренних сотрудников, так и у т работает за пределами организационной структуры).

Чем отличаются тестирование на проникновение

Об авторе

Евгений Архаров

В тестировании с 2010 года. Прошел путь от ручного тестировщика до руководителя отдела тестирования. В 2017 году решил сменить направление на автоматизацию и пришел в «Лабораторию качества» на должность тестировщика-автоматизатора. За это время автоматизировал несколько программных продуктов «с нуля».

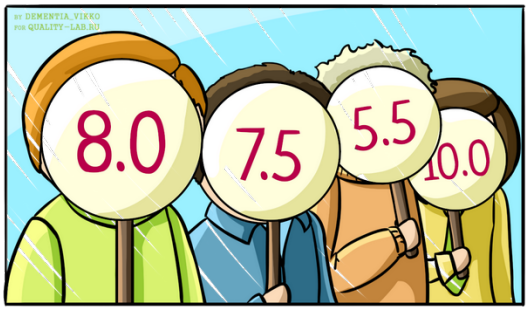
Поиск

Облако меток

8 марта (1) api (5) ISTQB FL (1)
IT (1) kpi (1)
kpi в тестировании (1) postman (1)
Quality lab. Meetup (2)
regress тестирование (1) rest api (2)
scrum (1) scrumban (1)
smoke тестирование (1)
soap api (1) sqa days (1) TDD (2)
UX-экспертиза (1) won't fix (1)
А/Б тестирование (1)
День дарения книг (1)
День защитника Отечества (1)
День рождения ЛК (1)
День смеха (1) Мероприятия (2)
ПОИНТ (3)
ие (1)
ания (1)
аудит (2) аудит тестирования (2)

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.

и оценка уязвимости?



Обе эти методики преследуют одну цель – сделать программный продукт безопасным, но имеют разные рабочие процессы.

Тестирование на проникновение – это проверка в реальном времени вручную или с помощью инструментов автоматизации; система и связанный с ней компонент подвергаются воздействию сэмулированных злонамеренных атак для выявления недостатков безопасности.

Оценка уязвимости включает в себя изучение и анализ системы с помощью инструментов тестирования с целью обнаружения лазеек в защите для нескольких вариантов вредоносных атак. Благодаря этой методике выявляются уязвимые области, которые могут предоставить хакерам возможность скомпрометировать систему. Кроме того, в процессе оценки уязвимости предусмотрены различные корректирующие меры, направленные на устранение выявленных недостатков.

Оценка уязвимости следует заранее определенной и установленной процедуре, в то время как тестирование на проникновение решает единственную задачу — разрушения системы вне зависимости от принятых подходов.

Для чего нужно тестирование на проникновение?

Как указывалось ранее, пробелы в безопасности обеспечивают неавторизованному пользователю или незаконному объекту возможность для атаки на систему, влияющей на ее целостность и конфиденциальность. Таким образом, тестирование программных продуктов на проникновение помогает избавиться от этих уязвимостей и сделать систему достаточно компетентной для защиты от ожидаемых и даже неожиданных вредоносных угроз и атак.

Рассмотрим результаты применения данной методики подробнее. Итак, тестирование на проникновение предоставляет:

- Способ выявления слабых и уязвимых областей системы еще до того, как их заметит хакер. Частые и сложные обновления системы могут повлиять на соответствующее оборудование и программное обеспечение, что приводит к проблемам безопасности, – следовательно, уместно контролировать все эти обновления.
- Возможность оценки существующего механизма безопасности системы. Это позволяет разработчикам оценить свою компетентность в защите и поддерживать уровень стандартов безопасности, установленный в системе. Помимо уязвимости системы рекомендуется также с помощью бизнес- и технической команд оценивать различные бизнес-риски и проблемы, включая любой компромисс с разрешенными и конфиденциальными данными организации. Это помогает организации структурировать и устанавливать приоритеты, смягчая или пол… исключая различные бизнес-риски и проблемы.
- Наконец (но не в последнюю очередь), инструмент для выявл… удовлетворения определенных основных стандартов, норм и практик безопасности.

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.

Как выполнить тестирование на проникновение?

Тестирование на проникновение системы может осуществляться с использованием любого из следующих подходов:

- ручное тестирование;
- автоматическое тестирование;
- сочетание ручного и автоматического тестирования.

1. Ручное тестирование на проникновение

Для проведения ручного тестирования на проникновение программного продукта используется последовательный стандартный подход, включающий следующие этапы:

- **Планирование тестирования проникновения.** Этот этап включает в себя сбор требований, определение сферы применения, стратегий и целей тестирования проникновения в соответствии с нормами безопасности. Кроме того, он может содержать оценку и перечисление проверяемых областей, типы планируемых испытаний и другие связанные с этим проверки.
- **Разведка.** Сбор и анализ максимально подробной информации о системных и связанных с ними атрибутах безопасности, полезных для таргетинга и атаки на каждый блок, для эффективного и результативного тестирования системы проникновения в систему. Различают две формы сбора и анализа информации о целевой системе: пассивная и активная разведка (в первом случае не предполагается прямое взаимодействие с системой).
- **Анализ уязвимости.** На этом этапе тестировщики выявляют и обнаруживают уязвимые области системы, которые в дальнейшем будут использоваться для входа и атаки с помощью тестов на проникновение.
- **Эксплуатация.** Фактическое испытание на проникновение в систему, включающее внутренние и внешние атаки. Внешние атаки – это сэмулированные атаки со стороны внешнего мира, преобладающие за пределами границы системы / сети (например, получение несанкционированного доступа к функциям и данным системы, относящимся к приложениям и серверам, обращенным к общественности). Внутренние атаки начинаются уже после вторжения авторизованных объектов в систему или сеть и имеют целью различные действия (при достижении компромисса с целостностью и правдивостью системы), которые способны преднамеренно или непреднамеренно скомпрометировать систему.
- **Пост-эксплуатация.** Следующий шаг – анализ каждой атаки на систему для оценки ее цели и задачи, а также ее потенциального воздействия на системные и бизнес-процессы.
- **Отчетность.** На самом деле, отчетность включает в документационную работу по мероприятиям, проводимым на упомянутых этапах. Кроме того, она может описывать различные риски, выявленные проблемы, уязвимые области (использованные или нет) и

специализация (2) с чего начать (2)
тест-анализ (2) тестирование (49)
тестирование безопасности (3)
тестирование для бизнеса (2)
тестирование мобильных приложений (2)
тестирование серого ящика (1)
тестирование требований (1)
тестирование черного ящика (1)
тестировщики (10)
тестовая документация (1)
тестовое покрытие (1) тесты (1)
техники тест-дизайна (1)
требования (1)
удаленная работа (1)
удобство использования (2)
управление проектами (4)
управление рисками (1) успехи (6)
целевая аудитория (3)
юзабилити (3)

Получите совет

Задайте вопрос нашему эксперту и владельцу компании

Ваше имя

Ваша Эл. почта

Ваш телефон

Ваш вопрос

☐ Я даю свое согласие на обработку персональных данных

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.

Перед отправкой необходимо разрешить обработку

предлагаемые для устранения недостатков решения.

персональных данных

2. Автоматическое тестирование на проникновение

Этот полезный и эффективный подход к проведению испытаний на проникновение предполагает использование специализированного инструментария. Автоматическое тестирование надежно, удобно, оно происходит очень быстро и легко поддается анализу. Инструменты проверки эффективны для точного обнаружения дефектов безопасности, присутствующих в системе, за короткий промежуток времени, а также для создания «кристально чистых» отчетов.

Назовем лишь некоторые из популярных и широко используемых инструментов тестирования на проникновение:

- Nmap;
- Nessus;
- Metasploit;
- Wireshark;
- OpenSSL;
- Cain & Abel;
- THC Hydra;
- w3af.

Многие инструменты для автоматизированного тестирования можно найти в готовых сборках Linux (Kali Linux, Mantra OS).

Для работы над конкретным проектом придется выбирать инструмент, отвечающий целому ряду требований и критериев:

- удобство развертывания, использования и обслуживания;
- обеспечение простого и быстрого сканирования системы;
- возможность автоматизации процесса проверки выявленных уязвимостей;
- доступность проверки ранее обнаруженных уязвимостей;
- способность создания простых и подробных отчетов об уязвимостях.

3. Сочетание ручного и автоматического тестирования на проникновение
Данный подход может быть признан оптимальным, так как он сочетает в себе преимущества первых двух вариантов и обеспечивает оперативный контроль с помощью надежного и точного проникновения в программный продукт.

Типы испытаний на проникновение

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.

Тестирование на проникновение в зависимости от используемых элементов и объектов может быть отнесено к следующим типам:

- **Социальная инженерия.** Тестирование с подключением «человеческого контингента», способного четко выявлять и получать конфиденциальные данные и другую информацию через Интернет или телефон (к этой группе могут относиться сотрудники организации или любые другие уполномоченные лица, присутствующие в сети организации).
- **Веб-приложение.** Используется для обнаружения прорех в безопасности и иных проблем в нескольких вариантах веб-приложений и сервисов, размещенных на стороне клиента или сервера.
- **Сетевая служба.** Тестирование проникновения в сеть для выявления и обнаружения возможности доступа хакерам или любому неавторизованному объекту.
- **Клиентская часть.** Как видно из названия, этот тест используется для тестирования приложений, установленных на клиентском сайте / приложении.
- **Удаленное подключение.** Тестирование vpn или аналогичного объекта, который может обеспечить доступ к подключенной системе.
- **Беспроводные сети.** Тест предназначен для беспроводных приложений и сервисов, включая их различные компоненты и функции (маршрутизаторы, фильтрационные пакеты, шифрование, дешифрование и т.д.).

Классифицировать тестирование на проникновение также можно и на основе используемых подходов к тестированию:

- **Белый ящик.** При таком подходе тестировщик будет иметь полный доступ к глубоким знаниям о функционировании и основных атрибутах системы. Это тестирование очень эффективно, так как понимание каждого аспекта системы очень полезно при проведении обширных испытаний на проникновение.
- **Черный ящик.** Тестировщикам предоставляется только высокоуровневая информация (например, URL или IP-адрес организации) для проведения тестирования на проникновение. Специалист может ощутить себя хакером, который ничего не знает о системе / сети. Это весьма трудоемкий подход, так как тестировщику требуется значительное количество времени для изучения свойств и деталей системы; кроме того, высока вероятность пропустить часть областей из-за недостатка времени и информации.
- **Серый ящик.** Тестировщик получает ограниченную информацию (например, знания алгоритма, архитектуры, внутренних состояний) для имитации внешней атаки на систему.

Ограничения тестирования на проникновение.

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.

У тестирования на проникновение существует ряд ограничений:

- недостаток времени и высокая стоимость тестирования;
- ограниченный объем испытаний, основанный на требованиях за данный период времени (что может привести к игнорированию других важных областей);
- возможность разрушения системы или потери системы в состоянии отказа в результате испытания на проникновение;
- уязвимость данных (потеря, коррупция или ущерб).

Вывод:

Хакеры, вооруженные усовершенствованными технологиями с широким спектром ресурсов и инструментов, зачастую легко врываются в систему или сеть с намерением причинить вред репутации и активам компании. Проверка на проникновение в большей мере, чем другие виды тестирования, может рассматриваться как инструмент выявления различных пробелов в безопасности, помогающий свести на нет потенциальные угрозы для системы в целом.

В завершение приведу несколько полезных ссылок.
Проект Awesome Penetration Testing постоянно обновляет инструменты, статьи, книги по тестированию на проникновение.

Стандарты:

- PCI DSS (Payment Card Industry Data Security Standard);
- OWASP (Open Web Application Security Project);
- ISO/IEC 27002, OSSTMM (The Open Source Security Testing Methodology Manual).

Сертификация:

- GPEN;
- Associate Security Tester (AST);
- Senior Security Tester (SST);
- Certified Penetration Tester (CPT).

процесс тестирования | тестирование | тестирование безопасности

© 2010—2022. Лаборатория качества

Екатерина Савинкина
Здравствуйте! Напишите мне, если у вас появятся вопросы.