Тестирование безопасности

Тестирование безопасности очень важно для защиты системы от вредоносных действий в сети.

Что такое тестирование безопасности?

Тестирование безопасности – это метод тестирования, позволяющий определить, защищает ли информационная система данные и поддерживает ли функциональность, как предполагалось. Тестирование безопасности не гарантирует полную безопасность системы, но важно включить тестирование безопасности как часть процесса тестирования.

Тестирование безопасности принимает следующие шесть мер для обеспечения защищенной среды:

- **Конфиденциальность** – защищает от разглашения информации непреднамеренным получателям.
- **Целостность** – позволяет передавать точную и правильную информацию от отправителей к получателям.
- **Аутентификация** – проверяет и подтверждает личность пользователя.
- **Авторизация** – определяет права доступа к пользователям и ресурсам.
- **Доступность** – обеспечивает готовность информации по требованию.
- **Безотказность** – гарантирует, что отправитель или получатель не получит отказа в отправке или получении сообщения.

Пример

Обнаружение недостатка безопасности в веб-приложении требует сложных шагов и творческого мышления. Иногда простой тест может подвергнуть самую серьезную угрозу безопасности. Вы можете попробовать этот самый базовый тест в любом веб-приложении –

- Войдите в веб-приложение, используя действительные учетные данные.
- Выйдите из веб-приложения.
- Нажмите кнопку НАЗАД браузера.
- Убедитесь, что вас попросили снова войти в систему или вы можете вернуться на страницу входа снова.

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Какие меры принимаются для обеспечения защищенной среды?
3. Заполните таблицу.

Таблица

Виды мер	Сущность принимаемых мер

Тестирование безопасности – процесс

Тестирование безопасности можно рассматривать как контролируемую атаку на систему, которая реалистично выявляет недостатки безопасности. Его цель – оценить текущее состояние ИТ-системы. Это также известно как **тест на проникновение** или более популярно как **этический взлом**.

Тест на проникновение проводится поэтапно, и здесь, в этой главе, мы обсудим весь процесс. Надлежащая документация должна быть сделана на каждом этапе, чтобы все шаги, необходимые для воспроизведения атаки, были легко доступны. Документация также служит основой для подробного отчета, который клиенты получают в конце теста на проникновение.

Тест на проникновение – рабочий процесс

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 тех, кто работает за пределами организационной структуры).

Практическое задание

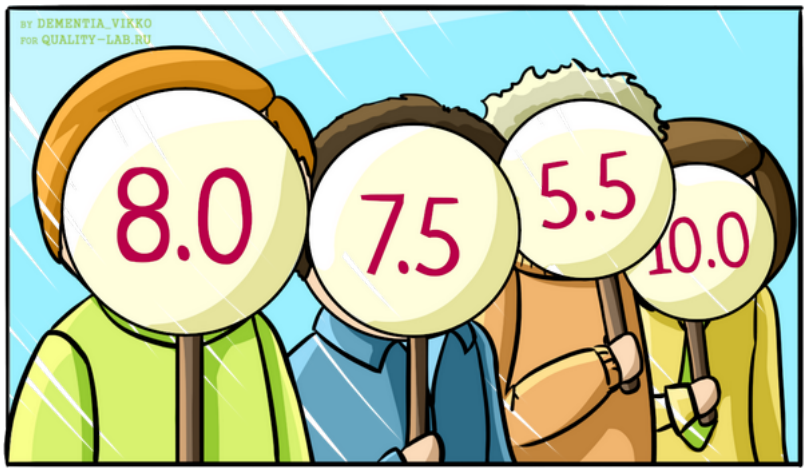
1. Проведите анализ предложенных информационных материалов.
2. Для чего необходимо документировать все этапы тестирования на проникновение?
3. Заполните таблицу.

Таблица

Проблемы в безопасности	Сущность проблем в безопасности

	отсутствие знаний и должной подготовки по вопросам безопасности как у внутренних сотрудников, так и у тех, кто работает за пределами организационной структуры
	безопасное подключение устраняет возможность вредоносных атак, а небезопасная сеть обеспечивает шлюз хакерам для нападения на систему
	ошибка, совершенная преднамеренно или непреднамеренно отдельным лицом или командой при проектировании, развертывании и обслуживании системы или сети
	например, недоработки в дизайне – один из наиболее важных факторов возникновения лазеек в безопасности
	контролировать механизм безопасности простой сетевой инфраструктуры легко, а отслеживать утечки или любую злонамеренную деятельность в сложных системах трудно
	неправильная или открытая передача конфиденциальных данных и информации среди команд или отдельных лиц

Чем отличаются тестирование на проникновение 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 полностью исключая различные бизнес-риски и проблемы.
- Наконец (но не в последнюю очередь), инструмент для выявления и удовлетворения определенных основных стандартов, норм и практик безопасности.

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Заполните таблицу, выписав сущностные характеристики двух процессов: оценка уязвимости и тестирование на проникновение.

Таблица

Оценка уязвимости	**Тестирование на проникновение**
изучение и анализ системы с помощью инструментов тестирования	помогает избавиться от этих уязвимостей
обнаружения лазеек в защите для нескольких вариантов вредоносных атак	помогает сделать систему достаточно компетентной для защиты от ожидаемых и даже неожиданных вредоносных угроз и атак
…	…

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 себя документационную работу по мероприятиям, проводимым на всех упомянутых этапах. Кроме того, она может описывать различные риски, выявленные проблемы, уязвимые области (использованные или нет) и предлагаемые для устранения недостатков решения.

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.

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Заполните таблицу, охарактеризовав все три подхода в тестировании на проникновение (ручное тестирование; автоматическое тестирование; сочетание ручного и автоматического тестирования).

Таблица

Ручное тестирование	**Автоматическое тестирование**	**Сочетание ручного и автоматического тестирования**
Включает следующие этапы:	Предполагает использование специализированного инструментария	Сочетает в себе…
	Эффективны для…	
…	…	…

Типы испытаний на проникновение

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.

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).

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Заполните таблицу, выписав типы и описание тестирований на проникновение.

Таблица

Типы тестирований	Описание
…	…

Тестирование безопасности – основы протокола HTTP

Понимание протокола очень важно, чтобы получить хорошее представление о тестировании безопасности.

Протокол HTTP

Протокол передачи гипертекста (HTTP) – это протокол прикладного уровня для распределенных, совместных, гипермедиа информационных систем. Это основа для передачи данных для Всемирной паутины с 1990 года. HTTP – это общий протокол без протокола состояния, который можно

использовать для других целей, а также с использованием расширения его методов запроса, кодов ошибок и заголовков.

По сути, HTTP – это протокол связи на основе TCP / IP, который используется для доставки таких данных, как файлы HTML, файлы изображений, результаты запросов и т. Д. Через Интернет. Он обеспечивает стандартизированный способ связи компьютеров друг с другом. Спецификация HTTP определяет, как запрашиваемые данные клиентов отправляются на сервер, и как серверы отвечают на эти запросы.

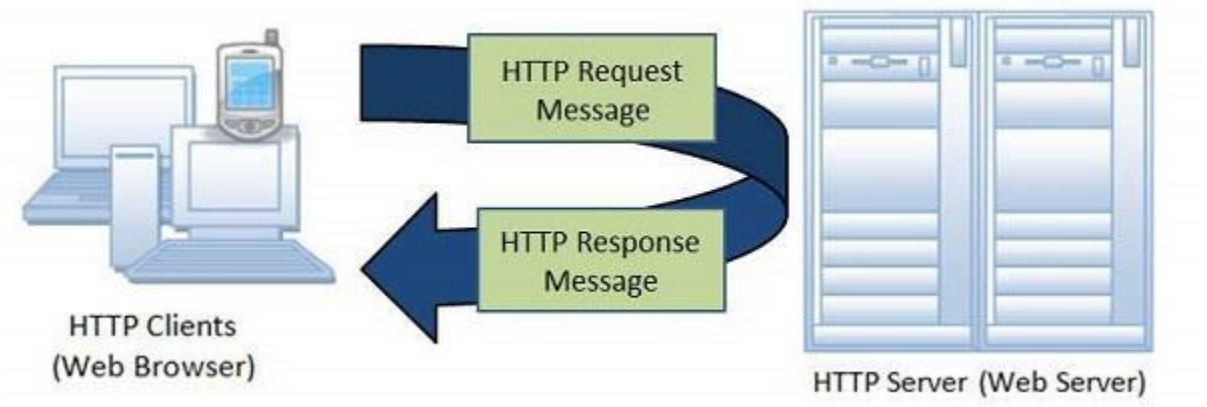
Основные характеристики

Существует три основных функции, которые делают HTTP простым, но мощным протоколом.

- **HTTP без установления соединения** – HTTP-клиент, т. Е. Браузер инициирует HTTP-запрос. После выполнения запроса клиент отключается от сервера и ожидает ответа. Сервер обрабатывает запрос и повторно устанавливает соединение с клиентом для отправки ответа обратно.
- **HTTP не зависит от носителя** – данные любого типа могут отправляться по протоколу HTTP, если и клиент, и сервер знают, как обрабатывать содержимое данных. Это необходимо как для клиента, так и для сервера, чтобы указать тип контента, используя соответствующий MIME-тип.
- **HTTP – без сохранения состояния** – HTTP **без** установления соединения, и это является прямым результатом того, что HTTP является протоколом без сохранения состояния. Сервер и клиент знают друг друга только во время текущего запроса. После этого они оба забывают друг о друге. Из-за этой природы протокола ни клиент, ни браузер не могут сохранять информацию между различными запросами на веб-страницах.

Архитектура

Следующая диаграмма показывает очень простую архитектуру веб-приложения и показывает, где находится HTTP –



Протокол HTTP – это протокол запроса / ответа, основанный на архитектуре клиент / сервер, где веб-браузер, роботы, поисковые системы и т. Д. Действуют как клиенты HTTP, а веб-сервер выступает в качестве сервера.

- **Клиент** – клиент HTTP отправляет запрос на сервер в форме метода запроса, URI и версии протокола, после чего следует сообщение,

подобное MIME, содержащее модификаторы запроса, информацию о клиенте и возможный контент тела через соединение TCP / IP.

- **Сервер** – HTTP-сервер отвечает строкой состояния, включая версию протокола сообщения и код успеха или ошибки, за которым следует MIME-подобное сообщение, содержащее информацию о сервере, метаинформацию объекта и возможное содержимое тела объекта.

HTTP – недостатки

- HTTP не является полностью защищенным протоколом.
- HTTP использует порт 80 в качестве порта по умолчанию для связи.
- HTTP работает на уровне приложения. Для передачи данных необходимо создать несколько соединений, что увеличивает накладные расходы на администрирование.
- Для использования HTTP не требуется шифрование / цифровые сертификаты.

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Заполните таблицу «Три основных функции HTTP-протокола»

Таблица

Функция	Описание

3. Нарисуйте две схемы:
   - В первой схеме отобразите действия клиента HTTP-протокола.
   - Во второй схеме отобразите действия сервера HTTP-протокола.

Пример:

Тестирование безопасности – Основы протокола HTTPS

HTTPS (протокол передачи гипертекста по протоколу Secure Socket Layer) или HTTP по SSL – это веб-протокол, разработанный Netscape. Это не протокол, а результат наложения HTTP поверх SSL / TLS (Secure Socket Layer / Transport Layer Security).

Короче говоря, HTTPS = HTTP + SSL

Когда требуется HTTPS?

Когда мы просматриваем, мы обычно отправляем и получаем информацию по протоколу HTTP. Так что это заставляет любого подслушивать разговор между нашим компьютером и веб-сервером. Много раз нам необходимо обмениваться конфиденциальной информацией, которую необходимо защитить и предотвратить несанкционированный доступ.

Протокол Https, используемый в следующих сценариях –

- Банковские сайты
- Платежный шлюз
- Торговые сайты
- Все страницы входа
- Приложения электронной почты

Основы работы HTTPS

- Открытый ключ и подписанные сертификаты требуются для сервера по протоколу HTTPS.
- Клиент запрашивает страницу https: //
- При использовании соединения https сервер отвечает на исходное соединение, предлагая список методов шифрования, поддерживаемых веб-сервером.
- В ответ клиент выбирает способ подключения, а клиент и сервер обмениваются сертификатами для проверки подлинности своих удостоверений.
- После этого и веб-сервер, и клиент обмениваются зашифрованной информацией, убедившись, что оба используют один и тот же ключ и соединение закрыто.
- Для размещения соединений https сервер должен иметь сертификат открытого ключа, который включает информацию о ключе с проверкой личности владельца ключа.
- Почти все сертификаты проверяются третьей стороной, так что клиенты уверены, что ключ всегда защищен.

Практическое задание

1. Проведите анализ предложенных информационных материалов.
2. Зарисуйте работу протокола HTTPS в виде схемы.