**Osint** – для создания карточки , Первый взгляд на компанию , сбор информаций. Имеет отношение one to many с классом Pentest для того чтобы не терять связь между классами .

***-- Имеет свой отчет –***

***-- Имеет место быть в отчете по пентесту для общей инфы –***

**Pentest –** Главный класс для отчета , в себе имеет информацию о компаний , доп документы по тесту , имеет .txt документы логов , логи берутся из консоли встроенной в интерфейс каждого документа класса. Есть проверки на базовые типы атак.

* **Pentest ( passive ) – Пасивная часть отчета “ Сбор информаций как можно больше”, имеет поля такие как :**
  1. **Название**
* **Pentest ( active ) – Активная чать теста ИС в которой проходит непосретсявенная попытка войти в систему , имеет поля такие как :**
  1. **Название**

***-- Имеет свой отчет –***

***-- Главная ось всего отчета –***

***Методолгий для пентеста.***

***OWASP***

***Open Web Application Security Project (OWASP)*** — открытое интернет-сообщество, которое предлагает самую исчерпывающую методологию для тестирования приложений, сайтов и API. Документация OWASP полезна любой ИТ-компании, которая заинтересована в создании безопасного программного обеспечения.

Одно из главных преимуществ OWASP в том, что методология описывает тестирование на каждой стадии жизненного цикла разработки приложений: определение требований, проектирование, разработка, внедрение и поддержка. При этом тестируются не только сами приложения, но и технологии, процессы, а также люди. Второе важное преимущество: OWASP могут применять как пентестеры, так и веб-разработчики.

**В последнем отчете OWASP перечислены 10 основных уязвимостей:**

1. Инъекции (Injections).
   * SQL Injection (SQLi):
   * Это тип инъекции, при котором злоумышленник внедряет вредоносные SQL-запросы в веб-приложение через входные данные, такие как формы на веб-сайте. Если приложение не корректно обрабатывает эти данные, злоумышленник может получить несанкционированный доступ к базе данных, изменять данные и даже удалить их.
   * Cross-Site Scripting (XSS):
   * Это тип инъекции, при котором злоумышленник внедряет вредоносный JavaScript код в веб-страницу, который будет выполнен в браузере других пользователей, просматривающих эту страницу. Это может привести к краже данных сессии, перенаправлению на злоумышленный сайт и другим атакам.
   * XML Injection:
   * Подобно SQL Injection, это инъекция, но в данном случае злоумышленник внедряет вредоносный XML-код в запросы и данных обмена данными между приложениями. Это может вызвать различные проблемы, включая обход аутентификации и доступ к чувствительной информации.
   * Command Injection:
   * В данном типе инъекции злоумышленник внедряет вредоносные команды в системные вызовы или исполняемые файлы на сервере. Это может привести к выполнению нежелательных действий на сервере, таким как удаление файлов, получение несанкционированного доступа и даже взлом сервера.
   * LDAP Injection:
   * Это инъекция, связанная с аутентификацией и авторизацией через LDAP-сервер. Злоумышленник пытается внедрить специальные символы и фильтры, чтобы обойти проверку подлинности и получить доступ к системе или данным.
   * NoSQL Injection:
   * Аналогично SQL Injection, этот тип инъекции связан с базами данных, использующими NoSQL-хранилища данных. Злоумышленник пытается внедрить вредоносные данные, чтобы получить доступ к базе данных и украсть или изменить информацию.
   * Server-Side Template Injection (SSTI):
   * Это инъекция, когда злоумышленник внедряет вредоносные команды или выражения в шаблоны, используемые на сервере для генерации динамического контента. Это может привести к выполнению нежелательных операций на сервере и утечке данных.
2. Нарушенная аутентификация (Broken Authentication).
   * Недостаточная или отсутствующая аутентификация: В некоторых приложениях может быть недостаточно механизмов аутентификации или они могут быть настроены неправильно. Это может позволить злоумышленникам обойти процесс аутентификации и получить доступ к учетным записям без ввода правильных учетных данных.
   * Ненадежное управление сессиями: Неправильное управление сессиями может привести к ситуациям, когда сессионные идентификаторы или данные аутентификации могут быть украдены или подделаны злоумышленниками. Это позволяет им сеансами аутентификации других пользователей.
   * Отсутствие времени ограничения сессии: Если сессии аутентификации не ограничены по времени и не завершаются после длительного бездействия пользователя, это может позволить злоумышленникам взять под контроль сеанс аутентификации, даже если пользователь покинул приложение.
   * Утечки информации о сессиях: В случае утечки данных о сессиях, таких как сессионные идентификаторы или данные аутентификации, злоумышленники могут использовать эти данные для манипуляции сессией и получения доступа к аккаунту пользователя.
   * Слабые пароли и недостаточная защита паролей: Если пользователи используют слабые пароли или хранят их в ненадежных местах, злоумышленники могут легко угадать или подобрать пароль и получить доступ к аккаунту.
3. Раскрытие критически важных данных (Sensitive Data Exposure).

* Недостаточное шифрование данных: Если данные, такие как пароли, личные и финансовые информация, передаются или хранятся в приложении без должного шифрования, они могут быть доступны злоумышленникам при перехвате трафика или в случае нарушения безопасности.
* Слабые алгоритмы шифрования: Использование слабых или устаревших алгоритмов шифрования может сделать данные уязвимыми к атакам на шифрование, таким как атаки методом перебора паролей.
* Хранение паролей в ненадежной форме: Если пароли хранятся в открытом виде или в ненадежно зашифрованном виде (например, в форме хешированных паролей без соли), злоумышленники могут легко получить доступ к аккаунтам пользователей.
* Отсутствие аутентификации при доступе к чувствительным данным: Некорректная аутентификация и авторизация при доступе к чувствительным данным может позволить несанкционированным пользователям получить доступ к этой информации.
* Отсутствие контроля доступа и надежной аутентификации API: Если API или интерфейсы приложения не имеют должного контроля доступа и аутентификации, злоумышленники могут обращаться к ним и получать доступ к данным.

1. Внешние объекты XML (XXE) (XML External Entities (XXE)).

* Внешние сущности XML: В стандарте XML существуют механизмы для определения внешних сущностей, которые могут быть использованы для подключения удаленных файлов, выполнения удаленных запросов и других действий.
* Некорректная фильтрация данных: Если приложение не фильтрует или не ограничивает внешние сущности, злоумышленник может внедрить вредоносные сущности в XML-документ и запустить различные виды атак.
* Удаленный доступ к файловой системе: Злоумышленник может использовать XXE, чтобы читать или записывать файлы на сервере, что может привести к утечке чувствительных данных или модификации системных файлов.
* Отправка запросов к внешним ресурсам: Атакующий может использовать XXE, чтобы отправлять запросы к удаленным ресурсам с сервера, на котором работает приложение, что может привести к дальнейшим атакам и утечке данных.
* Ускорение обработки данных: Некорректная обработка XXE-атак может вызвать отказ в обслуживании (DoS) приложения, так как атакующий может создавать большие и сложные XML-документы, которые будут тяжело обрабатываться.

1. Нарушенный контроль доступа (Broken Access control).
   * Недостаточное разделение ролей и прав: Ошибка в управлении ролями и правами пользователей может привести к тому, что пользователи могут выполнять действия, к которым у них нет прав доступа. Это может затронуть как администраторские функции, так и доступ к данным других пользователей.
   * Недостаточный контроль доступа к данным: Если приложение не обеспечивает надежное разделение данных между пользователями и позволяет им получать доступ к данным других пользователей, это может привести к утечке конфиденциальной информации.
   * Отсутствие защиты от повышения привилегий: Злоумышленники могут использовать уязвимости в приложении, чтобы повысить свои привилегии и получить доступ к функциям или данным, к которым они не имеют доступа.
2. Неправильная конфигурация безопасности (Security misconfigurations).
   * Открытые порты и службы: Незакрытые порты и службы на серверах могут предоставить злоумышленникам точку входа для атак. Это может произойти из-за недостаточных настроек брандмауэра или серверных служб, которые не должны были быть доступными извне.
   * Стандартные пароли и учетные записи: Если сервер или приложение используют стандартные пароли или оставлены с дефолтными учетными записями, это может легко использоваться злоумышленниками для несанкционированного доступа.
   * Недостаточная защита каталогов и файлов: Если директории и файлы на сервере доступны без ограничений, это может привести к утечке конфиденциальных данных, включая исходный код, конфигурационные файлы или логи.
   * Плохая настройка баз данных: Ошибки в настройке баз данных могут привести к неправильной видимости данных или открытию дверей для SQL-инъекций и других атак на базу данных.
   * Уязвимости в веб-приложениях: Неверная конфигурация параметров безопасности в веб-приложении, таких как отключенная защита от CSRF (межсайтовой подделки запросов), неправильная обработка сессий или недостаточные параметры контроля доступа, могут предоставить атакующим доступ к функционалу, которым им не следует обладать.
   * Утечка информации: Недостаточное скрытие деталей об ошибке или версиях используемого программного обеспечения может помочь злоумышленникам определить уязвимости и методы атаки.
3. Межсайтовый скриптинг (XSS) (Cross Site Scripting (XSS)).
   * Отраженный (Reflected) XSS: В этом виде XSS-атаки вредоносный код внедряется в URL или параметры запроса, и затем он отражается обратно на пользователя через веб-страницу. Атакующий отправляет жертве ссылку с вредоносным кодом, и если жертва переходит по этой ссылке, код выполняется в ее браузере.
   * Постоянный (Stored) XSS: Здесь вредоносный код сохраняется на сервере и отображается веб-страницей при каждом запросе к ней. Этот тип атаки может привести к постоянному исполнению кода на странице и воровству данных других пользователей.
   * DOM-based XSS: Этот вид XSS-атаки влияет на Document Object Model (DOM) браузера. Злоумышленник внедряет вредоносный код, который изменяет DOM и взаимодействует с веб-страницей на стороне клиента, что может привести к различным атакам.
   * Blind XSS: В случае "Blind XSS" атакующий может внедрить вредоносный код, но не видеть его результатов непосредственно. Вместо этого, он ожидает, что администраторы или другие авторизованные пользователи увидят результаты атаки, что делает ее менее заметной.
   * XSS через внешние ресурсы (XSS via External Resources): Этот вид XSS-атаки воздействует на сторонние веб-ресурсы, которые встроены в веб-страницу, такие как скрипты, стили или изображения. Злоумышленник может внедрить вредоносный код в такие ресурсы и заставить их выполняться на веб-странице.
4. Небезопасная десериализация (Insecure Deserialization).
   * Десериализация без проверки данных: Если приложение десериализует данные, полученные из ненадежных источников, без должной проверки и фильтрации, злоумышленники могут внедрить вредоносные данные, включая вредоносные объекты и код.
   * Выполнение вредоносного кода: Злоумышленники могут использовать небезопасную десериализацию для внедрения и выполнения вредоносного кода на сервере. Это может привести к удаленному выполнению кода (Remote Code Execution, RCE) и контролю над сервером.
   * Изменение данных: Злоумышленники могут модифицировать сериализованные данные и изменять хранимые данные на сервере. Это может привести к утечке, потере или повреждению данных.
   * Атаки на сессии и авторизацию: Небезопасная десериализация может быть использована для манипуляции данными сессии и авторизации, что позволяет атакующим получить несанкционированный доступ к учетным записям других пользователей.
   * Отказ в обслуживании (DoS): Злоумышленники могут использовать небезопасную десериализацию для создания больших и сложных данных, что может вызвать перегрузку сервера и отказ в его обслуживании.
5. Использование компонентов с известными уязвимостями (Using Components with known vulnerabilities).
   * Использование устаревших версий компонентов: Если разработчики используют старые версии сторонних компонентов или библиотек, это может означать, что они не включают последние исправления уязвимостей, которые были обнаружены и закрыты в более новых версиях.
   * Отсутствие мониторинга обновлений: Если разработчики не следят за обновлениями сторонних компонентов и библиотек, они могут упустить важные обновления безопасности.
   * Использование компонентов с известными уязвимостями: Злоумышленники могут анализировать структуру приложения и находить компоненты с известными уязвимостями. Затем они могут использовать эти уязвимости для атаки на приложение.
   * Утечка информации о версиях компонентов: Если приложение раскрывает информацию о используемых версиях компонентов, это может облегчить работу злоумышленникам, так как они будут знать, какие уязвимости могут быть использованы.
   * Каскадное воздействие: Уязвимость в одном компоненте может иметь каскадное воздействие на всё приложение, так как она может быть использована для атаки на другие компоненты или части системы.
6. Недостаточно подробные журналы и слабый мониторинг (Insufficient logging and monitoring).
   * Недостаточное журналирование событий: Если приложение не ведет подробные журналы событий, это затрудняет выявление и анализ потенциальных атак и инцидентов безопасности. Важные данные о запросах, ошибках, аутентификации и других действиях пользователей могут быть утрачены.
   * Отсутствие алармов и оповещений: Недостаточное мониторинга означает, что приложение может не реагировать на потенциально опасные события и не предоставлять администраторам информацию для принятия мер в случае атаки.
   * Задержка в обнаружении инцидентов: Если мониторинг проводится недостаточно активно или с задержкой, это может привести к потере времени на обнаружение и реагирование на инциденты, что увеличивает риск нанесения ущерба.
   * Недостаточное сохранение журналов: Если журналы хранятся недостаточно долго или удаляются слишком быстро, это может затруднить анализ прошлых событий и выявление долгосрочных атак.
   * Отсутствие аналитики безопасности: Недостаточно подробные журналы и слабый мониторинг делают невозможным проведение анализа безопасности и выявление необычной активности.

***ISSAF***

***Information System Security Assessment Framework (ISSAF)*** разработан Open Information Systems Security Group (OISSG). Документ охватывает большое количество вопросов, связанных с информационной безопасностью. В ISSAF приведены подробные рекомендации по тестированию на проникновение. Описаны утилиты, которыми можно провести пентест, указания по их использованию, а также подробно разъяснено, какие результаты и при каких параметрах можно получить в результате тестирования.

ISSAF считается достаточно сложной и подробной методологией, которую можно адаптировать для проверки информационной безопасности любой организации. Каждый этап тестирования согласно ISSAF тщательно документируется. Также даны рекомендации по использованию конкретных инструментов на каждом из этапов.

1. **Идентификация активов**: Определение всех информационных активов, включая данные, системы, оборудование и программное обеспечение, которые подлежат защите.
   1. Составление инвентаря активов: Составление полного списка всех активов организации, включая компьютеры, серверы, сетевое оборудование, программное обеспечение, данные, физические ресурсы и документацию.
   2. Классификация активов: Определение критичности каждого актива и его роли в работе организации. Например, определение, какие данные являются конфиденциальными, а какие - общедоступными.
   3. Оценка стоимости активов: Определение финансовой стоимости каждого актива, включая его приобретение, обслуживание и замену.
   4. Оценка уровня защиты: Оценка текущего уровня защиты каждого актива и определение, какие меры безопасности уже внедрены.
   5. Идентификация уязвимостей: Поиск уязвимостей в активах, которые могут стать объектом атак или угрожать их целостности и доступности.
   6. Документирование и классификация данных: Идентификация и классификация всех данных, которые обрабатываются в системе, включая конфиденциальные, личные и критически важные данные.
   7. Определение важных процессов: Определение ключевых бизнес-процессов, которые зависят от активов, и оценка влияния их недоступности или компрометации.
   8. Создание карты активов: Создание графической или текстовой карты, которая отображает расположение и связи между активами, а также их важность для организации.
2. **Оценка уязвимостей**: Поиск и анализ уязвимостей в системе, включая возможные точки входа для атак, неправильные настройки и слабые места.
   1. Сканирование активов: Идентификация всех активов в информационной системе, включая серверы, сетевое оборудование, приложения и базы данных.
   2. Использование сканеров уязвимостей: Использование специализированных инструментов и сканеров уязвимостей для обнаружения уязвимостей в системе. Эти инструменты могут проверять наличие необновленных программных компонентов, недостаточных настроек безопасности, открытых портов и других проблем.
   3. Анализ результатов сканирования: Оценка результатов сканирования для выявления и классификации уязвимостей по их серьезности и потенциальному воздействию на систему.
   4. Приоритизация уязвимостей: Установление приоритетов для устранения уязвимостей в зависимости от их критичности и возможности эксплойта. Некоторые уязвимости могут быть более критичными и требовать срочных мер по устранению.
   5. Разработка плана мероприятий: Создание плана действий для устранения уязвимостей. В плане должны быть определены сроки и ответственные лица за выполнение мероприятий.
   6. Проведение проверки уязвимостей: После принятия мер по устранению уязвимостей проводится повторная проверка для убедительности в успешности исправлений.
   7. Мониторинг уязвимостей: Регулярное отслеживание уязвимостей, так как новые уязвимости могут появляться с течением времени. Этот процесс включает в себя мониторинг обновлений программного обеспечения и систем.
   8. Обучение сотрудников: Обучение сотрудников в области информационной безопасности и о важности регулярной проверки и устранения уязвимостей.
3. **Оценка угроз**: Идентификация и оценка потенциальных угроз, которые могут повлиять на безопасность системы.
4. **Идентификация угроз**: Определите различные виды угроз, которые могут возникнуть для вашей информационной системы. Это могут быть угрозы как внутреннего, так и внешнего характера. Примеры угроз включают в себя несанкционированный доступ к данным, вредоносное программное обеспечение, физические угрозы (например, пожары или кражи) и многие другие.
5. **Оценка потенциальных ущербов**: Оцените, какой ущерб может быть причинен вашей организации в случае успешной реализации угрозы. Это может включать в себя финансовые потери, утрату репутации, юридические последствия и другие.
6. **Оценка вероятности**: Оцените вероятность возникновения каждой угрозы. Вероятность может быть высокой, средней или низкой, и она зависит от различных факторов, таких как история инцидентов, уровень защиты и другие.
7. **Ранжирование угроз**: Ранжируйте угрозы по их приоритетности. Это позволит организации сосредоточить усилия на наиболее критических угрозах.
8. **Разработка мер по смягчению рисков**: После оценки угроз разработайте меры по смягчению рисков. Это могут быть технические меры (например, использование брандмауэров и антивирусов), организационные меры (например, обучение сотрудников по правилам безопасности) и физические меры (например, установка системы контроля доступа).
9. **Постоянный мониторинг**: Угрозы и среда информационной безопасности постоянно меняются. Проводите регулярный мониторинг угроз и обновляйте меры по смягчению рисков в соответствии с изменениями.
10. **Создание плана реагирования на инциденты**: Разработайте план действий в случае реализации угрозы. Этот план должен включать в себя процедуры обнаружения инцидента, уведомления, изоляции и восстановления.
11. **Обучение персонала**: Обучите сотрудников организации об угрозах и плане реагирования на инциденты. Сотрудники должны знать, как действовать в случае возникновения угрозы.
12. **Аудит безопасности**: Проведите регулярные аудиты безопасности, чтобы убедиться, что меры по смягчению рисков эффективно работают и соответствуют текущим угрозам.
13. **Оценка политик и процедур безопасности**: Анализ документированных политик и процедур безопасности, чтобы убедиться, что они соответствуют стандартам и регуляторным требованиям.
    1. Идентификация существующих политик и процедур: Определите, какие политики и процедуры безопасности существуют в вашей организации. Это может включать в себя политики паролей, управления доступом, управления уязвимостями, защиты данных и другие.
    2. Анализ соответствия стандартам безопасности: Проверьте, соответствуют ли ваши текущие политики и процедуры стандартам безопасности, таким как ISO 27001, NIST SP 800-53 или другим соответствующим стандартам.
    3. Оценка эффективности: Оцените, насколько эффективно ваши политики и процедуры работают. Это включает в себя анализ и оценку реальных случаев нарушений безопасности, инцидентов и уязвимостей.
    4. Оценка актуальности: Удостоверьтесь, что политики и процедуры безопасности актуальны и соответствуют современным угрозам и технологиям. Они должны регулярно обновляться.
    5. Аудит безопасности: Проведите аудит политик и процедур безопасности с помощью внутренних или внешних экспертов. Это поможет выявить потенциальные недостатки и уязвимости.
    6. Обучение сотрудников: Обучите сотрудников вашей организации по соблюдению политик и процедур безопасности. Они должны быть осведомлены о том, как соблюдать установленные правила.
    7. Улучшение политик и процедур: На основе результатов оценки внесите необходимые изменения и улучшения в политики и процедуры безопасности. Это может включать в себя изменение политик, добавление новых процедур или усовершенствование текущих.
    8. Мониторинг и соблюдение: Установите системы мониторинга и контроля, чтобы убедиться, что сотрудники соблюдают политики и процедуры безопасности. Реагируйте на нарушения в соответствии с установленными процедурами.
    9. Реагирование на инциденты: Включите в политики и процедуры безопасности инструкции по реагированию на инциденты безопасности. Сотрудники должны знать, как сообщать о инцидентах и как действовать в случае их возникновения.
    10. Обновление и пересмотр: Политики и процедуры безопасности должны регулярно пересматриваться и обновляться в соответствии с изменениями в угрозах, технологиях и бизнес-процессах организации.
14. **Аутентификация и авторизация**: Проверка методов аутентификации и авторизации в системе для обеспечения правильной и безопасной идентификации и доступа пользователей.
    1. Идентификация методов аутентификации: Определите, какие методы аутентификации используются в вашей информационной системе. Это может включать в себя пароли, биометрическую аутентификацию, многофакторную аутентификацию и другие методы.
    2. Оценка сильности паролей: Проверьте, насколько сложны пароли, используемые пользователями. Пароли должны быть длинными, содержать буквы, цифры и специальные символы, и не должны быть легко угадываемыми.
    3. Оценка уровня доступа: Определите, какие пользователи имеют доступ к каким ресурсам и данные организации. Это может включать в себя определение ролей и привилегий пользователей.
    4. Проведение тестирования на проникновение: Попробуйте провести тестирование на проникновение, чтобы определить, насколько безопасна система относительно аутентификации и авторизации. Это может включать в себя попытку несанкционированного доступа и проверку, насколько сложно это сделать.
    5. Оценка многофакторной аутентификации: Если в системе используется многофакторная аутентификация, убедитесь, что она правильно настроена и работает корректно.
    6. Мониторинг и журналирование: Установите системы мониторинга и журналирования, чтобы отслеживать попытки несанкционированного доступа и другие события связанные с аутентификацией и авторизацией.
    7. Обучение сотрудников: Обучите сотрудников вашей организации по правилам безопасной аутентификации и авторизации. Они должны знать, как безопасно управлять своими учетными данными и доступом.
    8. Реагирование на инциденты: Включите в политики и процедуры инструкции по реагированию на инциденты связанные с нарушением аутентификации и авторизации.
    9. Обновление и улучшение: Периодически обновляйте методы аутентификации и авторизации в соответствии с современными стандартами и угрозами.
    10. Соблюдение стандартов безопасности: Убедитесь, что ваша оценка аутентификации и авторизации соответствует стандартам безопасности, таким как ISO 27001 или NIST SP 800-53.
15. **Мониторинг и обнаружение инцидентов**: Проверка механизмов мониторинга и обнаружения инцидентов для быстрого выявления аномальной активности и потенциальных нарушений.
    1. Оценка средств мониторинга: Определите, какие инструменты и системы мониторинга используются в вашей организации для отслеживания событий и инцидентов. Это может включать в себя системы журналирования, системы мониторинга безопасности (SIEM), средства анализа событий и другие.
    2. Идентификация целей мониторинга: Определите, какие цели и параметры мониторинга установлены в вашей организации. Что именно вы пытаетесь обнаружить и защитить?
    3. Анализ данных и журналов: Оцените, какие данные собираются и анализируются системами мониторинга. Это включает в себя анализ журналов событий, сетевой трафик, активность пользователей и другие данные.
    4. Оценка эффективности обнаружения: Оцените, насколько эффективно системы мониторинга способны обнаруживать инциденты безопасности. Могут ли они обнаружить аномальное поведение, атаки, вторжения и другие угрозы?
    5. Обучение персонала: Убедитесь, что сотрудники, ответственные за мониторинг и обнаружение инцидентов, обучены и компетентны в своей работе. Это включает в себя знание инструментов мониторинга и умение анализировать данные.
    6. Тестирование систем мониторинга: Проведите тестирование систем мониторинга с помощью симуляций инцидентов и атак, чтобы убедиться, что они работают корректно.
    7. Интеграция с системами реагирования: Убедитесь, что системы мониторинга интегрированы с системами реагирования на инциденты. Это позволит оперативно реагировать на обнаруженные угрозы.
    8. Оценка политик и процедур обнаружения инцидентов: Проверьте, какие политики и процедуры установлены для реагирования на обнаруженные инциденты. Оцените их соответствие стандартам безопасности.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте системы мониторинга и обнаружения инцидентов в соответствии с новыми угрозами и технологиями.
    10. Анализ инцидентов: Проведите анализ инцидентов, которые были обнаружены с помощью систем мониторинга, чтобы понять, какие меры безопасности могут быть улучшены.
16. **Контроль доступа**: Оценка системы контроля доступа, включая управление ролями, правами доступа и аудит доступа.
    1. Оценка средств мониторинга: Определите, какие инструменты и системы мониторинга используются в вашей организации для отслеживания событий и инцидентов. Это может включать в себя системы журналирования, системы мониторинга безопасности (SIEM), средства анализа событий и другие.
    2. Идентификация целей мониторинга: Определите, какие цели и параметры мониторинга установлены в вашей организации. Что именно вы пытаетесь обнаружить и защитить?
    3. Анализ данных и журналов: Оцените, какие данные собираются и анализируются системами мониторинга. Это включает в себя анализ журналов событий, сетевой трафик, активность пользователей и другие данные.
    4. Оценка эффективности обнаружения: Оцените, насколько эффективно системы мониторинга способны обнаруживать инциденты безопасности. Могут ли они обнаружить аномальное поведение, атаки, вторжения и другие угрозы?
    5. Обучение персонала: Убедитесь, что сотрудники, ответственные за мониторинг и обнаружение инцидентов, обучены и компетентны в своей работе. Это включает в себя знание инструментов мониторинга и умение анализировать данные.
    6. Тестирование систем мониторинга: Проведите тестирование систем мониторинга с помощью симуляций инцидентов и атак, чтобы убедиться, что они работают корректно.
    7. Интеграция с системами реагирования: Убедитесь, что системы мониторинга интегрированы с системами реагирования на инциденты. Это позволит оперативно реагировать на обнаруженные угрозы.
    8. Оценка политик и процедур обнаружения инцидентов: Проверьте, какие политики и процедуры установлены для реагирования на обнаруженные инциденты. Оцените их соответствие стандартам безопасности.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте системы мониторинга и обнаружения инцидентов в соответствии с новыми угрозами и технологиями.
    10. Анализ инцидентов: Проведите анализ инцидентов, которые были обнаружены с помощью систем мониторинга, чтобы понять, какие меры безопасности могут быть улучшены.
17. **Защита данных**: Проверка методов шифрования, защиты данных в покое и в движении, а также обработки конфиденциальных данных.
    1. Оценка средств мониторинга: Определите, какие инструменты и системы мониторинга используются в вашей организации для отслеживания событий и инцидентов. Это может включать в себя системы журналирования, системы мониторинга безопасности (SIEM), средства анализа событий и другие.
    2. Идентификация целей мониторинга: Определите, какие цели и параметры мониторинга установлены в вашей организации. Что именно вы пытаетесь обнаружить и защитить?
    3. Анализ данных и журналов: Оцените, какие данные собираются и анализируются системами мониторинга. Это включает в себя анализ журналов событий, сетевой трафик, активность пользователей и другие данные.
    4. Оценка эффективности обнаружения: Оцените, насколько эффективно системы мониторинга способны обнаруживать инциденты безопасности. Могут ли они обнаружить аномальное поведение, атаки, вторжения и другие угрозы?
    5. Обучение персонала: Убедитесь, что сотрудники, ответственные за мониторинг и обнаружение инцидентов, обучены и компетентны в своей работе. Это включает в себя знание инструментов мониторинга и умение анализировать данные.
    6. Тестирование систем мониторинга: Проведите тестирование систем мониторинга с помощью симуляций инцидентов и атак, чтобы убедиться, что они работают корректно.
    7. Интеграция с системами реагирования: Убедитесь, что системы мониторинга интегрированы с системами реагирования на инциденты. Это позволит оперативно реагировать на обнаруженные угрозы.
    8. Оценка политик и процедур обнаружения инцидентов: Проверьте, какие политики и процедуры установлены для реагирования на обнаруженные инциденты. Оцените их соответствие стандартам безопасности.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте системы мониторинга и обнаружения инцидентов в соответствии с новыми угрозами и технологиями.
    10. Анализ инцидентов: Проведите анализ инцидентов, которые были обнаружены с помощью систем мониторинга, чтобы понять, какие меры безопасности могут быть улучшены.
18. **Физическая безопасность**: Анализ физических мер безопасности, таких как ограничение доступа к серверам и сетевому оборудованию.
    1. Оценка доступа к физическим помещениям: Проверьте, какие меры предприняты для контроля доступа к физическим помещениям, где находятся серверы и оборудование, и убедитесь, что только авторизованные сотрудники имеют доступ.
    2. Оценка механизмов идентификации: Проверьте системы идентификации, такие как карточки доступа, биометрические средства, пин-коды и другие методы, используемые для определения легитимных пользователей.
    3. Мониторинг доступа: Убедитесь, что существует система мониторинга доступа, которая записывает события связанные с доступом к физическим помещениям, и способна обнаруживать несанкционированные попытки доступа.
    4. Оценка физической защиты оборудования: Проверьте, как оборудование, такое как серверы, сетевое оборудование и хранилища данных, физически защищены от несанкционированного доступа и воздействия.
    5. Пожарная безопасность: Оцените меры по обеспечению пожарной безопасности, такие как системы пожаротушения, детекторы дыма и системы оповещения в случае чрезвычайных ситуаций.
    6. Электропитание и бэкапы: Проверьте, как оборудование обеспечивается надежным и бесперебойным электропитанием, а также какие меры предприняты для резервного копирования данных.
    7. Обучение персонала: Обучите сотрудников вопросам физической безопасности, включая процедуры эвакуации и действия в случае чрезвычайных ситуаций.
    8. Аудит и проверка соответствия: Проведите аудит и проверку соответствия мерам физической безопасности, чтобы убедиться, что они соблюдаются.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте меры физической безопасности в соответствии с изменяющимися угрозами и требованиями.
19. **Обучение и осведомленность пользователей**: Оценка программ обучения пользователей и мер по повышению осведомленности в области информационной безопасности.
    1. Оценка доступа к физическим помещениям: Проверьте, какие меры предприняты для контроля доступа к физическим помещениям, где находятся серверы и оборудование, и убедитесь, что только авторизованные сотрудники имеют доступ.
    2. Оценка механизмов идентификации: Проверьте системы идентификации, такие как карточки доступа, биометрические средства, пин-коды и другие методы, используемые для определения легитимных пользователей.
    3. Мониторинг доступа: Убедитесь, что существует система мониторинга доступа, которая записывает события связанные с доступом к физическим помещениям, и способна обнаруживать несанкционированные попытки доступа.
    4. Оценка физической защиты оборудования: Проверьте, как оборудование, такое как серверы, сетевое оборудование и хранилища данных, физически защищены от несанкционированного доступа и воздействия.
    5. Пожарная безопасность: Оцените меры по обеспечению пожарной безопасности, такие как системы пожаротушения, детекторы дыма и системы оповещения в случае чрезвычайных ситуаций.
    6. Электропитание и бэкапы: Проверьте, как оборудование обеспечивается надежным и бесперебойным электропитанием, а также какие меры предприняты для резервного копирования данных.
    7. Обучение персонала: Обучите сотрудников вопросам физической безопасности, включая процедуры эвакуации и действия в случае чрезвычайных ситуаций.
    8. Аудит и проверка соответствия: Проведите аудит и проверку соответствия мерам физической безопасности, чтобы убедиться, что они соблюдаются.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте меры физической безопасности в соответствии с изменяющимися угрозами и требованиями.
20. **Планы восстановления после инцидента**: Оценка наличия и эффективности планов восстановления после инцидента и бизнес-планов продолжения деятельности.
    1. Оценка доступа к физическим помещениям: Проверьте, какие меры предприняты для контроля доступа к физическим помещениям, где находятся серверы и оборудование, и убедитесь, что только авторизованные сотрудники имеют доступ.
    2. Оценка механизмов идентификации: Проверьте системы идентификации, такие как карточки доступа, биометрические средства, пин-коды и другие методы, используемые для определения легитимных пользователей.
    3. Мониторинг доступа: Убедитесь, что существует система мониторинга доступа, которая записывает события связанные с доступом к физическим помещениям, и способна обнаруживать несанкционированные попытки доступа.
    4. Оценка физической защиты оборудования: Проверьте, как оборудование, такое как серверы, сетевое оборудование и хранилища данных, физически защищены от несанкционированного доступа и воздействия.
    5. Пожарная безопасность: Оцените меры по обеспечению пожарной безопасности, такие как системы пожаротушения, детекторы дыма и системы оповещения в случае чрезвычайных ситуаций.
    6. Электропитание и бэкапы: Проверьте, как оборудование обеспечивается надежным и бесперебойным электропитанием, а также какие меры предприняты для резервного копирования данных.
    7. Обучение персонала: Обучите сотрудников вопросам физической безопасности, включая процедуры эвакуации и действия в случае чрезвычайных ситуаций.
    8. Аудит и проверка соответствия: Проведите аудит и проверку соответствия мерам физической безопасности, чтобы убедиться, что они соблюдаются.
    9. Обновление и улучшение: Периодически обновляйте и улучшайте меры физической безопасности в соответствии с изменяющимися угрозами и требованиями.
21. **Аудит сети и сетевой безопасности**: Проверка конфигурации сети, обнаружение нежелательной активности и анализ сетевых протоколов.
22. **Идентификация активов**: Определите все активы сети, включая серверы, маршрутизаторы, коммутаторы, устройства пользователя и сетевые приложения.
23. **Идентификация и управление уязвимостями**: Проведите сканирование и анализ уязвимостей в сети. Оцените их серьезность и приоритет для устранения.
24. **Аутентификация и авторизация**: Проверьте, насколько эффективно реализованы меры аутентификации и авторизации в сети. Обратите внимание на слабые пароли, несанкционированный доступ и прочие нарушения.
25. **Контроль доступа**: Оцените меры контроля доступа, включая настройки прав доступа, роли и группы пользователей, а также механизмы аутентификации.
26. **Мониторинг сетевой активности**: Проверьте, насколько эффективно мониторится активность в сети. Обнаруживайте аномалии, несанкционированные действия и потенциальные инциденты безопасности.
27. **Защита от вредоносных программ и атак**: Оцените меры защиты от вредоносных программ, такие как антивирусное программное обеспечение и брандмауэры. Проверьте, какие меры предпринимаются для обнаружения и предотвращения атак, таких как DDoS и внедрение.
28. **Физическая безопасность**: Оцените физическую безопасность сетевых устройств, серверных комнат и дата-центров.
29. **Обновления и патчи**: Проверьте, насколько регулярно и эффективно обновляются операционные системы и прикладное программное обеспечение для закрытия уязвимостей.
30. **Резервное копирование и восстановление**: Оцените процедуры резервного копирования данных и планы восстановления после инцидента для обеспеч
31. **Соблюдение стандартов и регуляций**: Убедиться, что система соответствует требованиям стандартов и законодательства в области информационной безопасности
32. Оценка доступа к физическим помещениям: Проверьте, какие меры предприняты для контроля доступа к физическим помещениям, где находятся серверы и оборудование, и убедитесь, что только авторизованные сотрудники имеют доступ.
33. Оценка механизмов идентификации: Проверьте системы идентификации, такие как карточки доступа, биометрические средства, пин-коды и другие методы, используемые для определения легитимных пользователей.
34. Мониторинг доступа: Убедитесь, что существует система мониторинга доступа, которая записывает события связанные с доступом к физическим помещениям, и способна обнаруживать несанкционированные попытки доступа.
35. Оценка физической защиты оборудования: Проверьте, как оборудование, такое как серверы, сетевое оборудование и хранилища данных, физически защищены от несанкционированного доступа и воздействия.
36. Пожарная безопасность: Оцените меры по обеспечению пожарной безопасности, такие как системы пожаротушения, детекторы дыма и системы оповещения в случае чрезвычайных ситуаций.
37. Электропитание и бэкапы: Проверьте, как оборудование обеспечивается надежным и бесперебойным электропитанием, а также какие меры предприняты для резервного копирования данных.
38. Обучение персонала: Обучите сотрудников вопросам физической безопасности, включая процедуры эвакуации и действия в случае чрезвычайных ситуаций.
39. Аудит и проверка соответствия: Проведите аудит и проверку соответствия мерам физической безопасности, чтобы убедиться, что они соблюдаются.
40. Обновление и улучшение: Периодически обновляйте и улучшайте меры физической безопасности в соответствии с изменяющимися угрозами и требованиями.

***PTES***

***Penetration Testing Methodologies and Standards (PTES)*** предлагает рекомендации для проведения базового пентеста, а также несколько расширенных вариантов тестирования, для организаций с повышенными требованиями к информационной безопасности. Одно из преимуществ PTES в том, что он дает подробное описание целей и ожиданий от пентеста.

Основные этапы PTES:

* Обследование (Intelligence Gathering)
* Моделирование угроз
* Анализ уязвимостей
* Эксплуатация уязвимости
* Составление отчета

В PTES также содержится руководство по выполнению повторного, или постэксплуатационного, тестирования. Это помогает определить, насколько эффективно были закрыты выявленные уязвимости.

1. **Инициализация и согласование**: На этом этапе определяются цели и объем тестирования на проникновение, а также заключается соглашение с клиентом.
2. **Сбор информации и разведка**: Проводится сбор информации о целевой среде, включая активы, сетевую инфраструктуру и службы.
3. **Поиск уязвимостей**: Осуществляется сканирование и поиск уязвимостей в сети и системах.
4. **Анализ уязвимостей**: Выявленные уязвимости анализируются с точки зрения их серьезности и потенциального воздействия на безопасность.
5. **Эксплуатация**: Производится активная эксплуатация уязвимостей для получения доступа к системам и данным.
6. **Установка и удержание доступа**: С целью проверки уровня доступа и возможности сохранения контроля, на этом этапе устанавливаются механизмы удержания доступа.
7. **Сбор данных**: Осуществляется сбор данных и информации о целевой среде, включая конфиденциальные данные.
8. **Анализ данных**: Собранные данные анализируются и структурируются для выявления ценной информации.
9. **Уведомление и документирование**: Клиенту предоставляются результаты аудита, включая отчет о проведенных действиях и выявленных уязвимостях.
10. **Поддержка эксплуатации**: После завершения аудита, если это согласовано с клиентом, может предоставляться поддержка и рекомендации по устранению уязвимостей.
11. **Анализ результатов и документация**: Все действия, результаты и уязвимости документируются и анализируются.
12. **Отчет**: Подготавливается отчет о проведенном тестировании, включая выявленные уязвимости и рекомендации по их устранению.
13. **Завершение и очистка**: Тестирование завершается, и на всех целевых системах проводится очистка следов тестирования.
14. **Инициализация и согласование**: 1.1. Определение четких целей и ожиданий аудита. 1.2. Согласование методологии и инструментов, используемых во время аудита. 1.3. Установление расписания и сроков проведения аудита.
15. **Сбор информации и разведка**: 2.1. Поиск и сканирование активов, включая сетевые узлы и веб-ресурсы. 2.2. Анализ открытых портов и служб на целевых системах. 2.3. Исследование документации, доступной публично, связанной с организацией.
16. **Анализ уязвимостей и эксплуатация**: 3.1. Поиск уязвимостей в приложениях и системах. 3.2. Попытка эксплуатации уязвимостей для получения доступа. 3.3. Оценка реакции системы на атаки и проверка на возможность расширения доступа.
17. **Поддержание доступа и персистентность**: 4.1. Установка механизмов для поддержания доступа к системе после успешной эксплуатации. 4.2. Маскировка деятельности атакующего для избегания обнаружения. 4.3. Мониторинг активности и доступа к целевым ресурсам.
18. **Анализ данных и документация**: 5.1. Запись всех шагов аудита, включая найденные уязвимости и эксплуатацию. 5.2. Создание документации с описанием обнаруженных проблем и рекомендаций по устранению. 5.3. Формирование отчета о проведенном аудите с подробным анализом результатов.
19. **Завершение и передача результатов**: 6.1. Проведение встречи с клиентом для обсуждения найденных уязвимостей и рекомендаций. 6.2. Передача отчета о проведенном аудите и всех собранных данных клиенту. 6.3. Завершение проекта и закрытие аудита.
20. **Подготовка и планирование аудита**: 7.1. Определение целей и объема аудита на основе потребностей клиента. 7.2. Разработка детального плана аудита, включая выбор методологии и инструментов. 7.3. Назначение команды аудита и определение их ролей и обязанностей.
21. **Выполнение аудита и тестирование**: 8.1. Проведение активных тестов на проникновение, включая сканирование уязвимостей и эксплуатацию. 8.2. Сбор и анализ данных, связанных с обнаружением и анализом уязвимостей. 8.3. Тестирование политик безопасности, аутентификации и авторизации.
22. **Анализ результатов и формирование отчета**: 9.1. Обработка данных, полученных в результате тестирования и анализа уязвимостей. 9.2. Оценка уровня риска и потенциальных угроз для клиента. 9.3. Формирование подробного отчета о результатах аудита с рекомендациями по устранению уязвимостей.