

< Teach
Me
Skills />

PENTEST

Теория

Собираемся и отмечаемся

Вопросы по предыдущим темам или ДЗ

Mini-quizе по прошлым темам:

1. **Что такое OSINT?**
2. **Какие основные источники для OSINT?**
3. **Для чего проводить разведку по открытым источникам в сфере кибербеза?**
4. **Что является основой для безопасного и эффективного OSINT?**
5. **Какие могут быть негативные аспекты OSINT?**
6. **Какие принципы следует соблюдать при OSINT?**
7. **Какую информацию мы можем разыскать при помощи OSINT?**

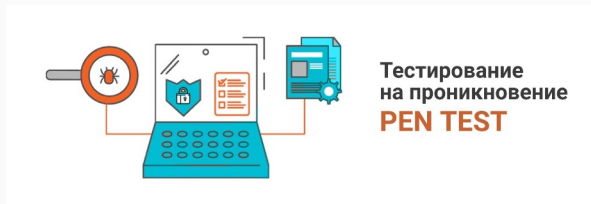
Mini-quizе по новой теме:

1. **Что такое «Пентест»? Как вы понимаете данное слово?**
2. **Как подразделяется Тестирование на проникновение?**
3. **Может ли при Пентесте применяться OSINT?**
4. **Из каких этапов должен состоять пентест?**
5. **Для чего применяется Пентест?**
6. **Могут ли применяться автоматизированные средства при пентесте?**
7. **Какие основные тенденции в тестировании на проникновение?**

План занятия

1. Рассмотрим что такое pentest, для чего он применяется.
2. Рассмотрим как его проводят, где и зачем.
3. Основные направления в тестировании
4. Так же рассмотрим основные тенденции и познакомимся с инструментами

Pentest (Пентест) — тестирование на проникновение, комплекс мер, которые имитируют реальную атаку на сеть или приложение.



Цель пентеста — понять, может ли злоумышленник взломать систему.

Пентест – санкционированный взлом. Топ-менеджмент компании может обозначить ключевые риски команде пентестеров при проведении работ, и те, в свою очередь, проверят на практике, как и при каких условиях риски могут быть реализованы. Эксперты дадут рекомендации, как настроить инфраструктуру и какие системы защиты использовать, чтобы устранить или минимизировать именно эти риски.

Пентест позволяет:

- ☐ Выявить слабые места, уязвимости в системах и сетях.
- ☐ Сформировать понимание, вектора атаки, способны ли злоумышленники нарушить работу системы; если да, то по какому вектору.
- ☐ Определить, как будет работать защита при разных хакерских атаках.
- ☐ Создать рекомендации, как можно исправить ситуацию.
- ☐ Предотвратить реальные хакерские атаки на системы.
- ☐ Сохранить безопасность и конфиденциальность данных и работоспособность сети.

Типы пентестеров

Этичный хакер, белый хакер, *white hat* — специалист по компьютерной безопасности, который специализируется на тестировании безопасности компьютерных систем. Он же «пентестер». В отличие от чёрных шляп (чёрных хакеров), белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищённым.

Типы хакеров



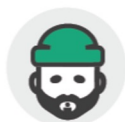
BLACK HAT
Хакер-преступник



WHITE HAT
Этичный хакер



GREY HAT
Не злой, но и не всегда этичный хакер



GREEN HAT
Хакер-новичок



BLUE HAT
Хакер-мститель



RED HAT
Хакер-линчеватель

По ролям:

Редтимеры (red teamers) — атакующие. Основная цель — проверить эффективность системы защиты и реакции персонала по обнаружению и предотвращению несанкционированного доступа.

Блютимеры (blue teamers) — защищающие. Их задача — обеспечивать защиту, укреплять безопасность, предотвращать атаки и реагировать на возникающие угрозы.

Анализ безопасности - метод, с помощью которого аналитики изучают, насколько устойчива внутренняя ИТ-инфраструктура к внешним или внутренним атакам. Это обеспечивает хороший обзор того, обеспечивает ли защитное кольцо организации поверхность атаки, и сколько потенциальных точек входа может найти злоумышленник. Анализ безопасности – начальный этап, он может служить отправной точкой для более углубленного тестирования, такого как «тестирование на проникновение».

Пентест показывает, в какой степени злоумышленник может проникнуть в инфраструктуру, в каком масштабе и как быстро он может нанести вред организации. Бывает, что достаточно одной точки входа, с помощью которой преступник может затем искать и находить более глубокие уязвимости, чтобы, наконец, добраться до настоящих информационных «сокровищ» компании. Пентест - обычно более трудоемкая задача, чем анализ безопасности, и более предпочтительный инструмент, когда речь идет о повышении осведомленности о безопасности в организации и предоставлении руководству более глубокого понимания реальных рисков для бизнеса.

Типы пентеста?

Критерий	Black Box	White Box
Определение	тестирование, как функциональное, так и нефункциональное, не предполагающее знания внутреннего устройства компонента или системы	тестирование, основанное на анализе внутренней структуры компонента или системы
Уровни, к которым применима техника	В основном: <ul style="list-style-type: none">• Приемочное тестирование• Системное тестирование	В основном: <ul style="list-style-type: none">• Юнит-тестирование• Интеграционное тестирование
Кто выполняет	Как правило, тестировщики	Как правило, разработчики
Знание программирования	Не нужно	Необходимо
Знание реализации	Не нужно	Необходимо
Основа для тест-кейсов	Спецификация, требования	Проектная документация

Так же можно отдельно выделить - **GreyBox** тестирование.

GreyBox - метод тестирования, в котором сочетаются элементы и черты Black Box и White Box пентестинга.

В GreyBox подходе пентестерам предоставляется частичная информация о системе, что делает этот метод более реалистичным и имитирует ситуацию, когда атакующий обладает некоторыми знаниями о целевой системе.

Так же можно отдельно выделить аппаратный пентест, программный, и социальный. Основным критерием является итоговая цель.

Типы тестирования

Белый ящик. Методика предполагает, что у пентестера есть знания о системе. Он может получить их от компании, для которой проводит тестирование. Тестировщик действует с учетом этих знаний. Помогает имитировать атаки от людей, которые смогли получить часть информации о продукте.

Преимущества:

- полный доступ к информации о системе;
- тестирование на всех уровнях;
- возможность оптимизации системы безопасности.

Недостатки:

- требуется полное участие заказчика;
- может занимать много времени;
- высокие затраты на подготовку и реализацию.

Черный ящик. У пентестера нет предварительной информации, он ведет себя как злоумышленник, который впервые столкнулся с системой. Он имеет данные, которые находятся в открытом доступе. Эту методику использует большая часть реальных взломщиков.

Преимущества:

- эмулирует реальные условия атаки хакера;
- позволяет оценить внешний уровень защиты системы;
- помогает провести независимое и объективное тестирование.

Недостатки:

- ограничено понимание внутренней структуры системы;
- риски упустить специфические уязвимости, для которых важно знать систему;
- бывают ложные срабатывания без уязвимостей.

Типы пентеста?

Сетевой пентестинг:

- *Внешний пентестинг.*
- *Внутренний пентестинг.*

Веб-приложения:

- *Тестирование на проникновение веб-приложений.*
- *Тестирование API.*

Физический пентестинг:

- *Физический доступ.*

Социальная инженерия:

- *Тестирование методик социальной инженерии.*

Беспроводной пентестинг:

- *Тестирование беспроводных сетей.*

Тестирование безопасности приложений:

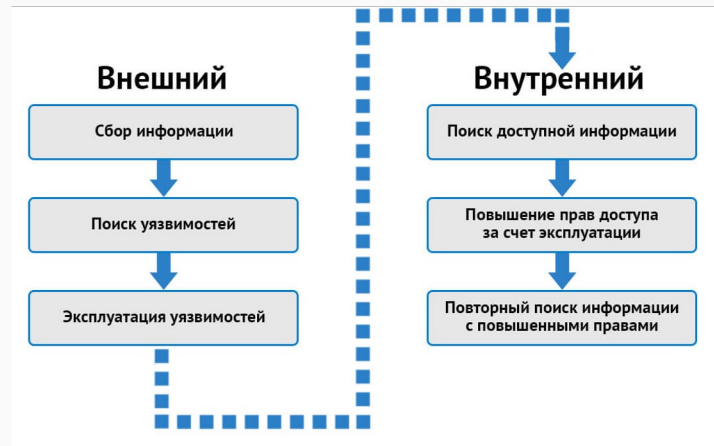
- *Тестирование мобильных приложений.*

Тестирование безопасности баз данных:

- *Тестирование СУБД.*

Исследование на предмет утечек информации:

- *Оценка утечек данных.*



Аппаратный пентест



Устройства класса - SDR или же SoftwareDefinedRadio - данное устройство представляет из себя радио, которое имеет широкий диапазон частот и возможность взаимодействия с ПК.



Различные модемы, устройства позволяющие перехватывать и атаковать Wi-Fi-сети. Так же они обеспечивают визуализацию Wi-Fi-ландшафта, мониторит и собирает данные о сети и устройствах в ней, и поддерживают атаки на WPA.



HID-устройства, позволяющие эмулировать HID устройства, предоставляя автоматизированный доступ и возможность управления устройством.

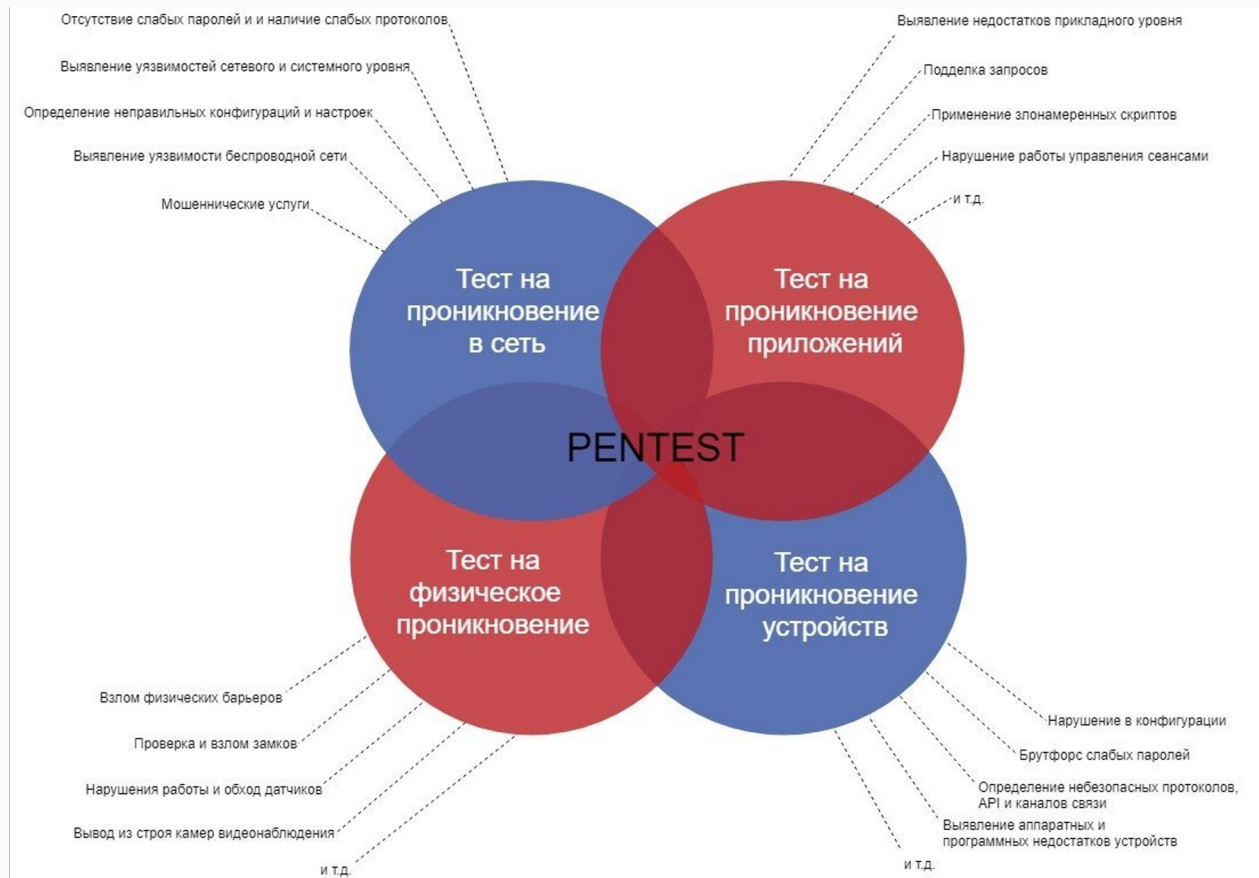
RFID-устройства, позволяющие прослушивать, дампить и записывать RFID-устройства, карты и прочее. Так же позволяют вносить изменения в созданные дампы.



Логический анализатор - прибор, который может записывать и отображать последовательности цифровых сигналов. Используется для тестирования и отладки цифровых и аналоговых устройств.



Как проводят пентест?



Burp Suite — это программное обеспечение безопасности, используемое для тестирования веб-приложений на проникновение.

OWASP ZAP - сканер безопасности веб-приложений с открытым исходным кодом.

MitmProxy - Mitmproxy — это набор инструментов, предоставляющих интерактивный перехватывающий прокси-сервер с поддержкой SSL/TLS для HTTP/1, HTTP/2 и WebSockets.

Metasploit. Metasploit Framework помогает создавать эксплойты — которые пользуются уязвимостями системы и проводят атаку. Metasploit позволяет анализировать уязвимости и создавать сигнатуры вирусов.

Nmap. Программа для сканирования сетей. Нужна для сбора сведений. Можно получить информацию о портах, о службах, об ОС на устройстве. Имеет GUI которое называется - zenmap.

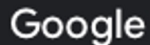
Nessus. Один из автоматизированных сканнеров. Помогает в поиске слабых мест. Имеет базу, которая обновляется каждую неделю. Nessus помогает автоматизировать поиск уязвимых участков сети и не выполнять ряд действий вручную.

Wireshark. Программа, которая анализирует трафик в сети. Позволяет анализировать различные протоколы и защищенный трафик в том числе.

Aircrack-ng. Программа нужна для обнаружения и перехвата трафика в беспроводных сетях. Помогает получить доступ к беспроводному адаптеру, проверить стойкость защиты, перехватить информацию из беспроводной сети.

BugBounty

Программа Bug Bounty — это программа, предлагаемая некоторыми веб-сайтами и разработчиками программного обеспечения, с помощью которой люди могут получить признание и вознаграждение за нахождение ошибок, особенно тех, которые касаются эксплойтов и уязвимостей.



Программа поиска уязвимостей от Google



HackerOne - платформа для поиска ошибок.



YesWeHack - одна из платформ для поиска и оплаты за нахождение багов.



BugCrowd - еще одна платформа для вознаграждений за уязвимости.

The logo for BugBountyBy, featuring a stylized icon of a hand pointing to the right and the text "BugBountyBy" in a bold, sans-serif font.

Инструментарий



Скрипт от FireEye - для ос на базе Win10/7 с инструментарием для проведения тестирования на проникновение, с большим количеством инструментов на базе .NET - очень удобный для тестирования инфраструктур на базе Windows.



Дистрибутив Debian - направленный на тестирование на проникновение. Имеет большое количество инструментов для проведения тестирования, как сетей, так и других операционных систем. Так же имеет в репертуаре некоторые фреймворке.



Дистрибутив на базе ArchLinux - нацеленный на тестирование на проникновение и оценку защищенности. Имеет в репертуаре большое количество инструментов. Имеет поддержку запуска с liveCD.

Компьютерные сети. Пентестер должен понимать, как устроена сетевая модель OSI, что это такое, каким образом функционируют компьютерные сети и где в них можно найти уязвимости. Необходимо знать протоколы, особенности их работы и типичные ошибки в настройках.

Операционные системы. При тестировании на проникновение необходимо работать с серверными и пользовательскими ОС. Поэтому тестировщик должен понимать, как они функционируют, причем на глубоком уровне. Потребуется изучить архитектуру и инфраструктуру, особенности процессов.

Криптография. Наука о шифровании информации, которая дает теоретические знания о том, как устроена защита сведений. Она знакомит с тем, как работают современные алгоритмы зашифровки и расшифровки, есть ли у них слабые места, как их можно найти.

Атаки на информационные системы. Это методы, которые применяют реальные злоумышленники. Пентестер должен знать и уметь их проводить, обходить системы безопасности и не быть обнаруженным.

Анализ вредоносного ПО. Пентестеры и специалисты по информационной безопасности должны знать о вирусах, трояках, червях, эксплойтах. Специалисту важно уметь написать вредоносное ПО под задачу и применить его.

Программирование. Чтобы писать скрипты и эксплойты, отдавать команды, нужно владеть как минимум одним языком программирования. Часто это системные языки. Ими пользуются, чтобы отдавать команды напрямую операционной системе. Но если пентестер знает несколько языков — это плюс. Например, Python для пентестера очень полезен.

Командная строка Linux. В основном пентестеры работают на специальных дистрибутивах Linux, поэтому должны хорошо владеть командной строкой ОС. Это бывает нужно и при имитации взлома.

Запрос на пентест / предварительное техническое задание

Любой планируемый проект начинается с технического задания на его выполнение.

Техническое задание в общем случае исходит от заказчика, но далеко не во всех случаях изначальный запрос на пентест содержит достаточно информации и все необходимые детали для планирования работ, которые в совокупности дают возможность ответить на основные вопросы - состав команды, трудоёмкость и сроки (в случае с внешним пентестом - цена, как зависимая величина)

В случае, если информации недостаточно (или это первичный запрос и ТЗ еще не сформировано) - заказчику высылается опросник.

Основные моменты к уточнению при предварительном планировании:

- необходимые виды работ (из типовых)
- количество и состав объектов
- для приложений - их функциональное назначение, архитектура (монолит/микросервисы) количество методов API
- для инфраструктуры - количество сервисов, основные виды сервисов
- цели, задачи, **особые требования**
- модели нарушителя (хотя бы в виде “ящиков” - какую информацию предоставят на старте?)
- требования к отчету по проекту
- необходимость проверки корректности исправления замечаний

Виды проектов по целям и задачам

- *Анализ защищенности* - работаем “на покрытие”

Акцент на выявление максимального количества уязвимостей и покрытие проверками всех объектов в скоупе (scope - периметр проверки - перечень объектов, подлежащих проверке, согласованный с заказчиком)

Рекомендации по устранению уязвимостей разрабатываются в стандартном (полном) объеме.

Анализ защищенности более характерен для пентеста приложений.

- *Тестирование на проникновение* - работа “на пробив”

Акцент на достижение заранее определенных целей взлома за отведенный период времени (получение админа домена, контроля/доступа к информации, достижение других заранее оговоренных целей)

Рекомендации могут не разрабатываться или предоставляться в базовом объеме.

Обычно используются все возможные средства, уязвимости раскручиваются до конца, получается вся возможная информация – полная имитация действий «злоумышленника».

Виды проектов по целям и задачам

- Тестирование на проникновение внешней инфраструктуры (реже - анализ защищенности)

Тестирование сервисов, доступных на внешнем периметре (включая веб-приложения - обычно на наиболее критичные уязвимости), вопрос о продвижении во внутреннюю сеть оговаривается отдельно

- Анализ защищенности веб-приложений (иногда - тестирование на проникновение)
 - без анализа исходного кода (черный/серый ящик)
 - включая анализ кода (белый ящик)
- Анализ защищенности мобильных приложений - Android, iOS
 - без анализа исходного кода (черный/серый ящик)
 - включая анализ кода (белый ящик)

Подробный анализ/тестирование одного или нескольких веб-приложений

- Тестирование на проникновение внутренней (локальной) IT-инфраструктуры (иногда - анализ защищенности)
 - через удаленное подключение
 - с выездом на площадки заказчика

Виды проектов по целям и задачам

- Анализ защищенности/тестирование на проникновение беспроводных сетей

Выезды на площадки, анализ WiFi, попытки пробиться

- Тестирование осведомленности персонала в отношении атак с применением методов социальной инженерии

Фишинг, вишинг отдельным проектом (в составе редтиминга делается по умолчанию)

- Реагирование на инциденты/Расследование инцидентов

Кого-то взломали, просят 1) выкинуть хакеров из систем 2) найти как было взломано 3) проверить все остальное

- Нагрузочное тестирование (устойчивость к DoS/DDoS)

Прежде чем начинать тестирование, необходимо заключить письменное соглашение между пентестером и компанией / организацией / частным лицом, чтобы определить рамки пентеста и уточнить все вопросы, касающиеся безопасности данных, раскрытия и т. д.,

Ключевые положения договора:

1. Предмет договора (вид работ, общая информация об объектах со ссылкой на техзадание, “Заказчик поручает провести”)
2. Сроки, этапы, порядок старта работ (в особо формальных случаях прописывается необходимость авторизационное письма от заказчика)
3. Обязательства заказчика по предоставлению доступов и информации (привязка старта работ и сроков к получению доступов и информации, конкретные требования к предоставляемым доступам и инфо - обычно в техзадании)
4. Порядок приемки работ (конкретные требования к форматам и составу отчетности - обычно в техзадании)
5. Порядок оплаты
6. Порядок работы с конфиденциальной и прочей информацией, обязательства обеих сторон
7. Обязательства и ответственность пентестеров в отношении доступности систем, сохранности информации (нас в основном интересует адекватное ограничение такой ответственности)
8. Заверения заказчика о том что все объекты принадлежат ему наличии права проводить пентест на объектах (желательно - но практически никогда нет в договорах, можно прописывать в “Предмете договора”)

Описание объектов и конкретные требования к пентесту и отчетности обычно выносятся в техническое задание - приложением к договору (такая форма удобна в том числе для разделения ответственности по согласованию договора - юристы отвечают за общую часть, =производство (пентестеры) - за детали техзадания.

9. Техническое задание (требования к деталям технического исполнения, методике)

- Объекты с детализацией (скоуп, ака периметр проверки)
- Сроки, календарный план
- Конкретные условия начала работ, что именно предоставляет заказчик для старта
- Описание работ, применяемые методики, модели нарушителя (информация может быть разной степени детализации - от списка общепринятых стандартов до чеклиста с конкретными действиями - пентестерам лучше меньше детализации)
- Особые требования к проведению работ (немедленное предоставление информации о критических уязвимостях, необходимость согласования или запрет определенных действий, ограничение нагрузки на узлы и т.п)
- Порядок расширения периметра проверки, включения дополнительных объектов (или положение о том, что расширение скоупа не предусмотрено)
- Требования к текущей и финальной отчетности (содержание, форматы, необходимость/периодичность предоставления статуса по работам)

Основной результат деятельности пентестера – **Отчет**.

1. Описание проекта
2. виды работ
3. Скоуп (периметр проверки) - объекты
3. Методика.

Общая часть - результаты

4. Резюме и общая оценка защищенности (низкая-средняя-высокая).
“Резюме для руководства”
5. Перечень всех замечаний с указанием оценки (таблица: номер-наименование-оценка-объекты)
6. Общие рекомендации по устранению/митигации (снижение влияния) недостатков.

Специальная часть

Здесь приводятся все замечания, каждое включает подробное описаниеб структурированное следующим образом:

1. Заголовок, краткая суть, узлы/объекты.
2. Степень опасности (низкая-средняя-высокая).
3. Подробное описание уязвимости/недостатка.
4. Демонстрация наличия уязвимости и возможности ее эксплуатации.
5. Рекомендации.

Приложения

7. Перечень скомпрометированных узлов, учетных данных, информации к которой получен доступ.
8. Перечень внесенных изменений – залитые файлы, созданные/измененные учетные записи, изменения в настройках.

Скриншоты

Снимки экрана являются важной составляющей при составлении заметок и технических отчетов. Хороший скриншот может объяснить обсуждаемый вопрос с первого взгляда и более подробно, чем текстовое описание. Особенно полезны скриншоты для представления технически сложного или насыщенного деталями раздела отчета. Как говорится, картинка стоит 1000 слов. И наоборот, плохой скриншот может затуманить и отвлечь внимание от сути проблемы.

Хороший скриншот обладает следующими характеристиками:

- разборчивость
- содержит визуальные признаки того, что он относится к клиенту
- содержит описываемый материал
- поддерживает описание материала
- правильно оформляет описываемый материал.

Сравнение методик

Covered issues	PTES	OSSTMM	NIST	ISSAF	OWASP
Разработка и постановка целей пентеста	+	+	+/-	+	+
Подготовка договора	+/-	+	+/-	+	-
Правовые вопросы (в основном ориентировано на США)	-	+/-	+	+	-
Сбор информации	+	+	+	+	+
Анализ и оценка уязвимостей	+	+/-	+/-	+	+
Этапы тестирования	+	+	+	+	+
Тестирование сети	+	+	+	+	+/-
Тестирование WiFi	+	+	+	+	-
Тестирование веб-приложений	+	+/-	-	+/-	+
Тестирование физических активов	+	+	-	+	-
Тестирование безопасности паролей	+	-	+	+	+/-
Тестирование безопасности баз данных	-	-	-	+	+/-
Тестирование безопасности кода	-	-	-	+	+/-
Отчетность	+	+	-	+	+
Рекомендации по смягчению последствий	-	-	+	+	-

Penetration Testing Execution Standard - PTES

Здесь вы можете скачать актуальную версию PTES v1.1 <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

Представляет из себя собой рекомендуемый подход к структуре тестирования на проникновение.

В дополнение к руководству для пентестеров, в PTES также содержится информация для бизнеса о том, что они должны ожидать от теста на проникновение для помощи в определении объема и согласовании проектов.

PTES состоит из двух основных частей, которые дополняют друг друга:

1. Стандарт выполнения тестирования на проникновение, описывающий основные разделы и этапы тестирования на проникновение
2. Техническое руководство, в котором обсуждаются конкретные инструменты и техники, которые должны быть использованы на каждом этапе.

Penetration Testing Execution Standard

PTES качестве стандарта официально зарегистрирован только в США.

С момента появления стандарт получил развитие в виде версии 1.1 в 2017 г.

Стандарт **PTES** предусматривает 7 основных этапов проведения тестирования на проникновение, описанных в соответствующих разделах:

1. Этап первоначального общения
2. Сбор информации
3. Моделирование угроз
4. Анализ уязвимостей
5. Эксплуатация
6. Постэксплуатация
7. Отчетность

The Open Source Security Testing Methodology Manual - [OSSTMM]

Ссылка на PDF <https://www.isecom.org/OSSTMM.3.pdf>

The Open Source Security Testing Methodology Manual (OSSTMM) - руководство по методологии тестирования безопасности с открытым исходным кодом

OSSTMM охватывает следующие ключевые моменты:

- Анализ безопасности
- Метрики операционной безопасности
- Анализ доверия
- Рабочий поток
- Тестирование человеческой безопасности
- Тестирование физической безопасности
- Тестирование безопасности беспроводных сетей
- Тестирование безопасности телекоммуникаций
- Тестирование безопасности сетей передачи данных
- Регламенты соответствия
- Отчетность с помощью STAR (Security Test Audit Report)

NIST SP 800-115

В руководстве описаны три основных метода оценки:

- Тестирование - выполнение технических тестов на целевых сетях и системах.
- Экспертиза - основной процесс нетехнической оценки, заключающийся в проверке, инспектировании, обзоре, наблюдении, изучении или анализе.
- Интервью - еще один метод нетехнической оценки, описываемый как процесс проведения дискуссий с отдельными лицами или группами в организации для облегчения понимания, получения разъяснений или определения местонахождения доказательств.

NIST SP800-115 делит проект оценки безопасности на три фазы:

- Планирование охватывает начальные этапы проекта, такие как сбор информации, идентификация активов и моделирование угроз.
- Выполнение в основном сосредоточено на поиске уязвимостей системы, сети и организационных процессов.
- После выполнения проводится оценка найденных ранее уязвимостей и их влияния.

Information System Security Assessment Framework (ISSAF) - методология Open Information Systems Security Group (OISSG).

Методика **ISSAF** – Information System Security Assessment Framework разработана консорциумом OISSG (Open Information Systems Security Group) в качестве стандарта внутреннего аудита организаций этого консорциума.

ISSAF предусматривает следующие мероприятия по аудиту аспектов ИБ:

1. Оценка политик и процедур ИБ организации, а также степень их соответствия ИТ-стандартам и требованиям нормативных документов в области ИБ
2. Выявление и оценка «зависимости» бизнес-процессов организаций от ИТ-инфраструктуры
3. Проведение оценки уязвимостей и тестов на проникновение для выделения уязвимостей в системе, которые могут привести к потенциальным рискам информационных ресурсов
4. Указание моделей оценки по доменам безопасности
5. Нахождение и устранение неправильных конфигураций аппаратно-программных средств
6. Идентификация и снижение рисков, связанных с ИТ
7. Идентификация и снижение рисков, связанных с персоналом или бизнес-процессами
8. Усиление безопасности существующих процессов и технологий
9. Внедрение лучшего опыта обеспечения ИБ в практику и процедуры бизнес-процессов

OWASP methodologies

Open Web Application Security Project® (OWASP) это известная некоммерческая организация, которая работает над повышением безопасности программного обеспечения. OWASP зарегистрирована в США и Бельгии (OWASP Europe VZW)

Среди всего, что они создали, есть набор руководств и методик по тестированию безопасности под названием The OWASP Testing Framework.

В него входят их собственные методики:OWASP Testing Guides:

- Web Security Testing Guide (WSTG)
- Mobile Security Testing Guide (MSTG)
- Firmware Security Testing Methodology

https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies



OWASP

Open Web Application
Security Project

MITRE ATT&CK™.

<https://attack.mitre.org>

MITRE ATT&CK™ представляет собой постоянно развивающийся центр руководств, тактик и техник злоумышленников, используемых ИТ-отделами и службами безопасности для определения рисков организации, расстановки приоритетов и концентрации усилий по защите. Он помогает командам кибербезопасности оценить эффективность процессов и защитных мер их операционного центра безопасности (SOC), чтобы определить области для улучшения. Это хорошая база знаний для аналитика по безопасности. Одна из самых популярных методик среди специалистов по кибербезопасности.

Основная цель - составление политик безопасности. Она не ориентирована на проведение пентестов, но из нее можно почерпнуть много полезных деталей.

ATT&CK

Методика BSI

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile&v=1

Методика **BSI** – Study a Penetration Testing Model разработана немецкой государственной организацией Federal Office for Information Security. В этой методике подробно описываются не только последовательность проведения тестов, но и необходимые требования по ИБ, а также правовые аспекты тестирования на проникновение.

Материал методики **BSI** организован в следующие разделы:

1. ИТ-безопасность и тесты на проникновение;
2. объекты тестов на проникновение и их классификация;
3. правовые вопросы;
4. общие требования;
5. методика проведения тестов на проникновение;
6. выполнение тестов на проникновение.

Согласно методике **BSI**, выделяется три основных типа воздействий:

1. Атаки через сеть;
2. Атаки с применением социальной инженерии;
3. обход физических мер безопасности.

MindMapy для пентеста внутренней инфраструктуры (AD)

<https://orange-cyberdefense.github.io/ocd-mindmaps/>

https://orange-cyberdefense.github.io/ocd-mindmaps/img/pentest_ad_dark_2023_02.svg

<https://i.ibb.co/TKYNCNP/Pentest-ad.png>

https://blog.marcolancini.it/images/posts/blog_hackerplaybook_mindmap.png

Дефолтные учетные записи различных вендоров

- 1 APC apc apc
- 2 Asus admin password
- 3 Asus admin admin
- 4 Brocade admin password
- 5 Cisco cisco cisco 192.168.10.2
- 6 Cisco admin admin 192.168.1.1
- 7 Cisco cisco cisco 192.168.1.1
- 8 Cisco cisco cisco 192.168.1.254
- 9 Cisco admin admin 192.168.1.254
- 10 Cisco Ironport admin ironport 192.168.42.42
- 11 HP admin admin 192.168.1.1
- 12 HP admin password 192.168.1.2
- 13 Huawei Admin admin 192.168.1.1
- 14 Huawei admin admin 192.168.1.1
- 15 Huawei user user 192.168.1.1
- 16 Huawei root Huawei12#\$
- 17 Huawei Administrator Admin@9000
- 18 kali root toor
- 19 kali kali kali
- 20 Linksys admin admin 192.168.1.1
- 21 Linksys [none] admin 192.168.0.1
- 22 TrendMicro admin admin

[Статья по поиску инфы в интернете](#)

DuckDuckGo: это поисковая система браузера Tor по умолчанию .
Главным преимуществом DuckDuckGo являются его функции конфиденциальности. Поскольку он не отслеживает пользователей, люди могут использовать его для анонимного просмотра темной сети.

Путешествие по даркнету

Burp Academy (Web)

- <https://portswigger.net/web-security>

For Beginners

- <https://play.picoctf.org/>
- <https://247ctf.com>
- <https://angstromctf.com>

Reversing

- <http://reversing.kr> - регистрация только с VPN проходит
- <https://io.netgarage.org>
- <https://challenges.re>

Binary Exploitation

- <https://overthewire.org/wargames/>
- <https://pwnable.tw>
- <https://pwnable.xyz>

WEB

- <http://websec.fr>
- <https://webhacking.kr>
- <https://owasp.org/www-project-juice-shop/>
- <https://ctf.hacker101.com/>
- <https://xss-game.appspot.com>
- <http://google-gruyere.appspot.com>
- <https://www.hackthissite.org>
- [http://webappsecmovies.sourceforge.net/webg
oat/](http://webappsecmovies.sourceforge.net/webg
oat/)

Mix

Mobile apps

- <https://www.ragingrock.com/AndroidAppRE/>
- <https://github.com/xtiankisutsa/awesome-mobile-CTF>

Уязвимые виртуальные машины

- <https://www.hackthebox.eu/>
- <https://www.root-me.org/>
- <https://www.cyberseclabs.co.uk> - только VPN
- <https://pwn.college>
- <https://ctflearn.com>
- <http://www.hacker.org/challenge/> - ошибка (возможно дело в ВПН)
- <https://ringzer0ctf.com/challenges>
- <https://hbh.sh/home>
- <https://w3challs.com>
- <https://ctf.hackucf.org/challenges>
- <http://ctf.infosecinstitute.com/index.php> - вроде работает но криво
- <https://hack.me>
- <https://www.cybergamesuk.com/code-crackers>
- <https://atenea.ccn-cert.cni.es/home>
- <https://www.hacking-lab.com/> - триал
- <https://ctftime.org/>
- <https://exploit-exercises.com>
- <https://w3challs.com/>
- <https://www.pentesterlab.com/exercises/> - платный

Спасибо за внимание!