**Основные понятия**

Что же такое «пентест» или «тестирование на проникновение»? Если обратиться к Википедии:

«**Тестирование на проникновение** (жарг. *пентест*) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании».

Таким образом, **пентест** — это некий объёмный процесс, который помогает понять фактическую защищённость какой-то сетевой системы и выявить места, уязвимые для действий злоумышленников.

В зависимости от целей тестирования, применяется различный набор техник с разной агрессивностью. В одном случае предполагается просто нахождение уязвимостей без дальнейшей их эксплуатации и проникновения внутрь периметра. В других случаях, естественно, по договорённости с заказчиком, возможно применение грубой силы вплоть до брутфорса или социальной инженерии.

Иногда тестируется отдельный сервис, а иногда тестированию может подвергнуться мобильное приложение (не путать с реверсом). Процесс тестирования должен быть чётко оговорён с заказчиком (в виде договора) или регламентом (если организация проводит тестирование самой себя). Отсутствие условий (или рамок) пентеста может привести к незапланированной недоступности критических для организации сервисов и финансовым потерям (или, например, социальная инженерия напугает рядовых сотрудников).

**Основная задача пентеста** — выявление уязвимых мест (с точки зрения нападающего) и способов их эксплуатации в условиях, очерченных рамками договора или регламента, чтобы в дальнейшем их устранить и повысить уровень защищённости системы.

**Логичным итогом пентеста** является **отчёт** с подробным описанием обнаруженных недочётов системы и действий, которые привели к реализации атак, и рекомендациями по устранению найденного.

Многие ошибочно считают, что простое сканирование с применением популярного (возможно, даже сертифицированного по требованиям законодательства РФ) сканера уязвимостей (инструмента автоматизированного анализа уязвимостей) вроде *Nessus*, *MaxPatrol*, *Acunetix* и других и есть пентест. Но это является заблуждением, потому что автоматизированное сканирование не может дать надёжного результата хотя бы потому, что у всех сканеров (скорее всего) результаты будут отличаться процентов на 20, ввиду разных баз уязвимостей, разного подхода к сканированию, а также *false positive* (ложно-положительных) реакций.

Полноценный пентест подразумевает не только автоматизированный, но и ручной поиск уязвимого места и плюсом предполагает доказательство найденных уязвимостей через их эксплуатацию.

**Эксплуатация уязвимости** — получение доступа, повышение привилегий, выполнение каких-либо неожиданных для тестируемой системы операций.

**Привилегии** — права на совершение каких-либо действий в системе.

**Эскалация привилегий** — повышение уровня доступа к ресурсам системы, которое достигается за счёт эксплуатации её уязвимости. Другими словами, получение расширенных прав в системе.

Мало найти уязвимость сканером, надо её проэксплуатировать и доказать, что это опасная уязвимость. В общем случае автоматическое сканирование и поиск уязвимостей могут применяться как вспомогательное средство для периодической оценки уровня защищённости системы самим заказчиком или на начальных этапах пентеста.

**Модель безопасности**

Существуют разные схематические представления модели безопасности (пирамиды, колёса и т.д.). На рисунке 1 визуально представлена такая модель безопасности, как пирамида (не путать с *security triangle*!).

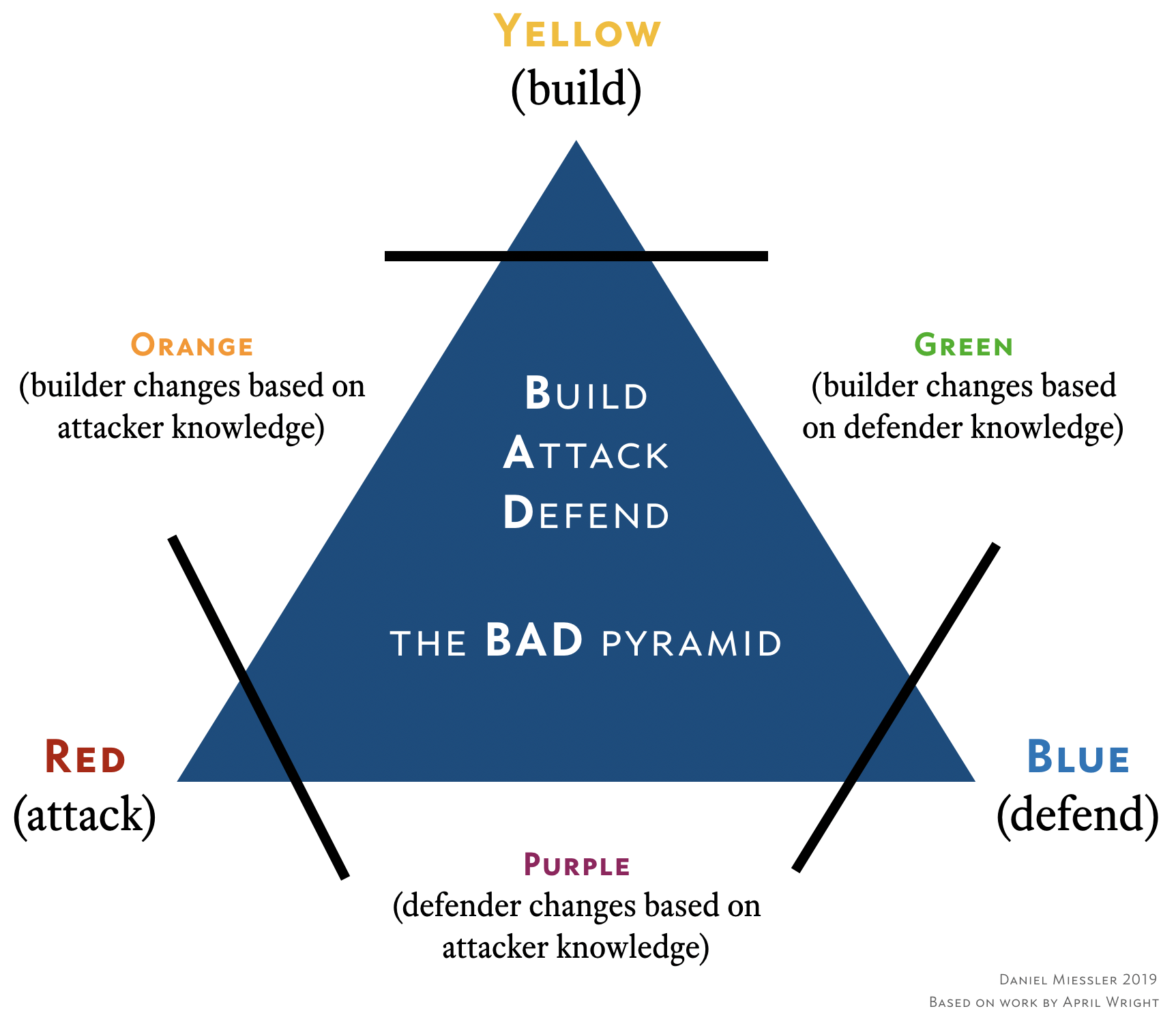


Рисунок 1. Модель безопасности в виде пирамиды. Источник: [danielmiessler.com](https://danielmiessler.com/images/BAD-pyramid-miessler.png)

Но мы рассмотрим модель в виде колеса *infosec wheel* как более наглядную. Но так как блоки информации соотносятся друг с другом в обеих моделях, узнаем подробнее о месте специалистов по пентесту в информационной безопасности.

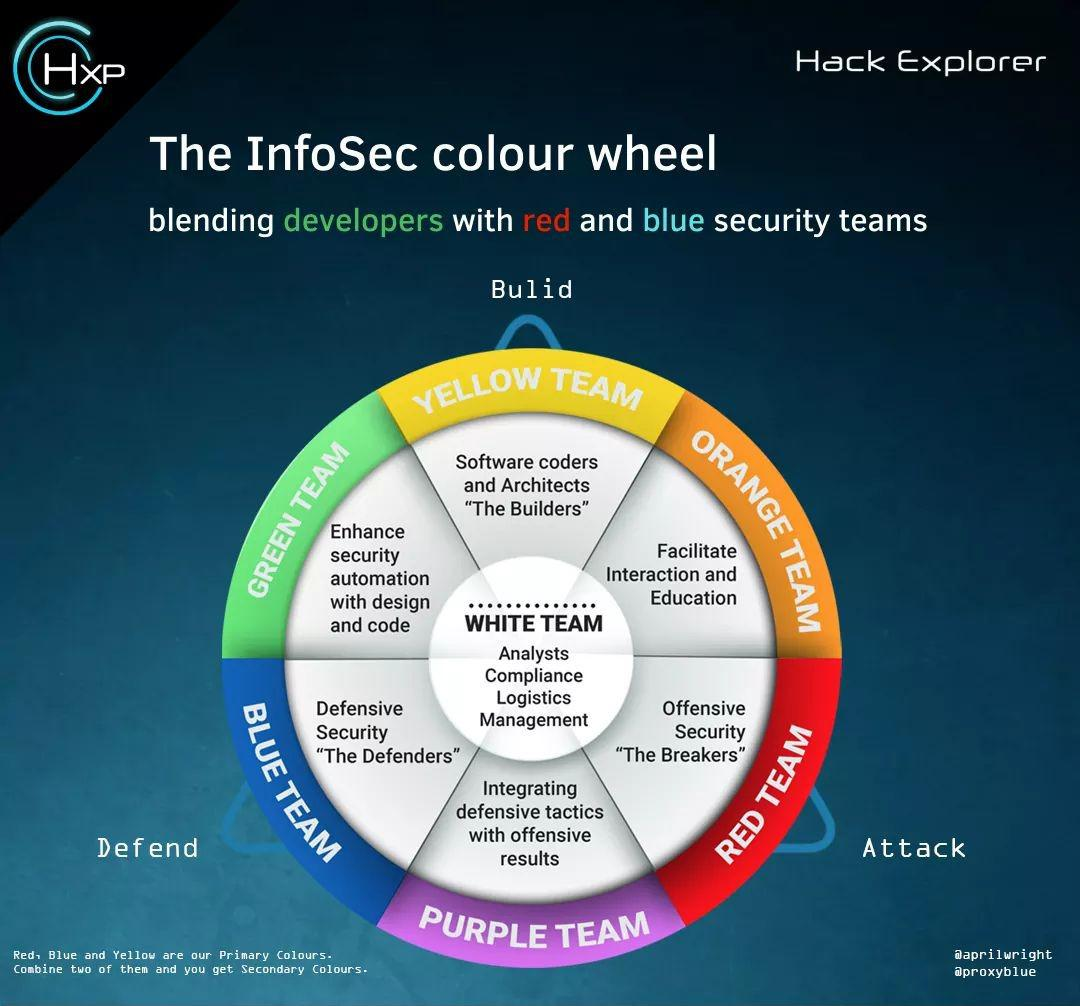


Рисунок 2. Модель безопасности *infosec wheel*. Источник: [hackernoon.com](https://cdn.hackernoon.com/images/f2apxyNoEZUNnwGm1NG6OQfqlJA2-p3236r9.jpg)

**Infosec wheel**

Информационная безопасность организации, как правило, опирается на две команды специалистов — красную (*red team*) и синюю (*blue team*). Цветовое обозначение пошло ещё от американских военных, которые делились на две команды: красную — нападающие (или атакующие), синюю — защищающиеся (или обороняющиеся).

В плане особенностей функций *red team* нападает извне, пытается всячески найти и проэксплуатировать уязвимости, а *blue team* строит всякие заборы, укрепляет сервисы и ставит ловушки на атакующих. В процессе обучения наши действия будут ближе к действиям *red team* команд, хотя деятельность *blue team* мы тоже рассмотрим.

Разработчики также участвуют в развитии информационных систем организации, они постоянно пишут обновления в систему и выводят их в эксплуатацию, а значит, открывают всё новое и новое поле для деятельности красной и синей команд. И в этих разработках нужно не забывать про безопасность.

Так появляются новые цвета в нашем *infosec wheel* — жёлтый (это сами разработчики), зелёный и оранжевый — это уже некий симбиоз безопасности с разработкой. И наиболее яркий пример этому — всё большая популярность специалистов *DevSecOps* (с 2018 года, до РФ вот как раз дошли тенденции).

**DevSecOps** — это важное направление в *DevOps* (наборе практик, нацеленных на взаимодействие разработчиков ПО с экспертами по безопасности), подразумевающее обеспечение безопасности на всех этапах разработки приложений.

Как показывает практика, организации, внедряющие безопасность в жизненный цикл ПО, демонстрируют лучшие результаты в обеспечении ИБ. Подробнее можете прочитать в [статье](https://www.securitylab.ru/news/500357.php).

И тут возникает ещё больше направлений безопасности (помимо тестирования на проникновения и постройки заборов), а именно — статический и динамический анализы кода и интеграция подходов безопасности в среду разработки. Это помогает избежать долгого и кропотливого тестирования уже готовой системы на выходе в эксплуатацию и постоянно на любом билде (версии или каких-то новых модулях системы) поддерживать высокий уровень безопасности.

Основная сложность при разработке чего-то нового или расширении возможностей существующей системы — это балансировать между безопасностью, функциональностью и простотой интерфейса.

**Задание 1.2.1**

1/1 point (graded)

Выберите верный ответ на вопрос: к деятельности каких пентестеров относится настройка межсетевых экранов и авторизации в сервисах?

*red team*

*blue team*

*yellow team*

верно

Ответ

Верно:

В их обязанности входит поддержание высокого уровня защищённости сервисов.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

Для этого существует модель безопасности — **security triangle** (треугольник безопасности), условное представление состояния системы.

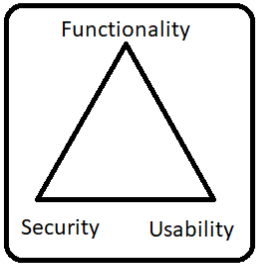


Рисунок 3. *Security triangle*. Источник: [greycampus.com](https://www.greycampus.com/ckeditor_assets/pictures/295/content_SFU.triangle.PNG)

Если мы поставим точку внутри треугольника в любом месте (это будет маркер состояния нашей системы), то сможем соотнести уровни безопасности, функциональности и удобства пользования.

Работает это так: чем ближе точка к *security*, тем ниже функциональность. Передвигая точку внутри треугольника, мы будем изменять состояние этих трёх параметров.

Например, мы хотим сделать банковское приложение, соответственно, нам нужен максимально высокий уровень безопасности (понятно, зачем?), и мы перемещаем точку в угол *security*, получаем максимальный уровень безопасности и никакой функциональности (кроме одной кнопки «Перевести деньги», например). И потребительские качества сервиса будут низки.

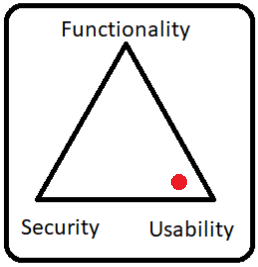
Чем больше мы добавляем «плюшек» и уходим в сторону функциональности, тем сложнее обеспечить безопасность и разобраться пользователю (как раз *usability*).

*Infosec wheel* затрагивает только «легальных» безопасников, то есть специалистов, профессионально занимающихся вопросами безопасности на основании договора (трудового или договора подряда, к примеру).

Но есть ещё одна классификация специалистов по безопасности (а именно, хакеров), которая называет всех шляпами (*hat*) и делит так же по цветам.

**Задание 1.2.2**

1/1 point (graded)



Выберите верное утверждение, описывающее параметры системы по треугольнику безопасности:

Низкий уровень безопасности, низкий уровень функциональности, высокая простота использования

Красная точка в сетевой инфраструктуре

Низкий уровень безопасности, большое количество разнообразных функций, минималистичный интерфейс с одной кнопкой

Низкая функциональность приложения, высокая защищённость системы, простой интерфейс для пользователя

верно

Ответ

Верно:

Судя по расположению точки в треугольнике безопасности, мы видим, что в этой системе может быть минимум функций, отсутствие шифрований, но её очень легко использовать, лёгкий, красивый и приятный интерфейс.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Классификация хакеров: white hat, black hat, grey hat**



Рисунок 4. Типы хакеров. Источник: [bitnoticias.com.br](https://bitnoticias.com.br/wp-content/uploads/2019/01/Hackers.jpg)

В этой классификации специалисты делятся на профили *White hat*, *Black hat*, *Grey hat*. Поговорим о каждом подробнее.

**White hat**

*White hat* (они же «белые шляпы», «белые шапки» и другие вариации в сообществе) — это профессиональные хакеры, только те, которые работают на хороших парней, чтобы помочь решить любые национальные или корпоративные проблемы.

**Black hat**

*Black hat* («чёрные шляпы», «блэчить» от слова «*black*» — перейти на тёмную сторону) — полная противоположность «белых шляп». Это хакеры, которые пишут вредоносные программы, занимаются взломом компьютеров, систем и веб-сайтов, приложений. Они представляют угрозу кибербезопасности, могут выкрасть персональные данные и иную важную информацию, проводят атаки *DDoS* и прочее. И образ таких плохих парней возникает в голове при слове «хакеры», в том числе благодаря СМИ.

Хакеры *Black hat* работают только на то, чтобы нанести вред потенциальным жертвам, вымогать деньги или уничтожать программное обеспечение на их устройствах. Хакеры *Black hat* — это те, кто нарушает кибербезопасность в злонамеренных целях, что приводит к краже данных или финансовым потерям для пострадавших.

**Grey hat**

Роль специалистов профиля «серой шляпы» — среднее между тем, что делает *Black hat*, и тем, что делает *White hat*. Это гибкие профессиональные хакеры, которые доступны для большинства за отдельную плату. Например, хакер *Grey hat* поможет организации поймать злоумышленников за определённую сумму. С другой стороны, он также возьмётся за проект взлома организаций в интересах атакующих, но тоже за оплату. Он может использовать уязвимость, а затем довести её до сведения организации. Дело в том, что это незаконно — взламывать чьё-либо устройство без официального разрешения, поэтому хакеры *Grey hat* находятся на пограничной линии, балансируя между хорошими и плохими парнями.

Если с профилями по цветам всё более-менее понятно, то стоит сказать об отдельных категориях хакеров, действующих, исходя из разных соображений, но всегда как злоумышленники.



Рисунок 5. *Script kiddie*. Источник: [cyberhoot.com](https://cyberhoot.com/wp-content/uploads/2019/12/script-kiddie-1024x442-1.png)

Самой популярной и разрушительной категорией является *Script kiddie* («детишки со скриптами») — неквалифицированные хакеры, которые полагаются на сторонние программы и скрипты для ведения кибератаки на компьютерные сети, системы и веб-сайты. Это может быть как ребёнок, так и взрослый человек, но чаще всего это пользователь компьютера в подростковом возрасте, который не знает об этических принципах профессиональных хакеров либо же их полностью отвергает, т. е. он хочет власти хакера без дисциплины и обучения. У него нет стремления к получению знаний, мотивов к самообразованию и уважения к навыкам. Он использует готовые программы для взлома, фишинга, фрикинга и других форм электронного хаоса, даже не зная, как они работают, что делают и для чего созданы.

Есть ещё менее распространённые, но также опасные категории хакеров:

* *Suicide hackers* — «хакеры-суицидники», абсолютно не задумывающиеся о последствиях своих действий.
* *Cyber terrorists* — идейные хакеры, ломающие что-то из своих убеждений и во имя своих целей (не финансовых).
* *Hacktivists* — хакеры, чья основная цель — привлечь к себе максимальное внимание и славу, но не в Инстаграме, а совершая крупные акции, направленные (как правило) на государственные организации по всему миру. Уровень выше *Script kiddie*, но и амбиций больше.

**Подведём итог**

На курсе мы будем заниматься именно легальным тестированием на проникновение, то есть этичным хакингом, который существует на основании закона и договорённостей с организациями. Разновидностей такой деятельности тоже достаточно много, как и методологий. Изучим их в следующем юните.

**Задание 1.2.3**

1/1 point (graded)

Основная задача пентеста — это:

Выявление уязвимых мест и способов их эксплуатации с целью дальнейшего устранения и повышения уровня защищённости системы в условиях, очерченных рамками договора или регламента

Автоматизированное сканирование системы, выявление уязвимостей и их эксплуатация

Эскалация привилегий в системе и произведение неожиданных для системы действий с целью выявления уязвимостей

Повышение привилегий в системе с целью сбора персональных данных и получения конфиденциальной информации

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Задание 1.2.4**

1/1 point (graded)

К какому типу хакеров относятся кардеры (*carders*)?

*Script kiddie*

*White hat*

Это не хакеры, это мошенники с платёжными системами

Cпециалисты по тестированию безопасности в банковской сфере

верно

Ответ

Верно:

Это преступники, ворующие данные платёжных карт и обналичивающие их (или покупающие на них какие-то товары в интернет-магазинах, могут использовать некоторые приемы хакеров *Black hat*, но хакерами не являются).

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Ваш вопрос по теме юнита**

0 points possible (ungraded)

*Напишите вопрос в поле ниже:*

Code Editor



1

нету вопросов

Чтобы выйти, нажмите ESC и затем TAB или щёлкните вне редактора кода.

верно

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

Мы уже ознакомились с наиболее популярными цветами и оттенками, существующими в мире кибербезопасности, но на этом цветовая индикация не заканчивается.

Основные варианты легального тестирования системы (сети, сайта, чего угодно) тоже удобно различать по цветовым профилям.

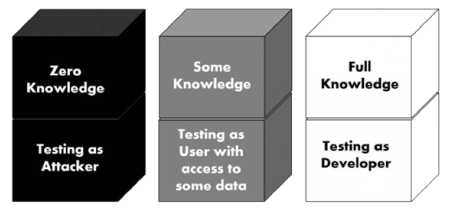


Рисунок 6. Методы тестирования. Источник: [devopedia.org](https://devopedia.org/images/article/76/6522.1547742539.jpg)

Существует **три типа тестирования** (кстати, у тестировщиков ПО примерно так же), которые отличаются по уровню знаний о тестируемых системах:

* **Black box** — тестирование ведётся вслепую с минимальными знаниями вроде общедоступных данных (сайт, название организации, адрес, телефон).
* **White box** — вы обладаете всеми данными на систему (исходные коды, админский доступ и т.д.).
* **Grey box** — вы обладаете частичными знаниями о системе (например, у вас есть учётная запись пользователя без привилегий, вы знаете, что в организации есть какие-то информационные системы, но не знаете, где они и как работают).

Эти виды тестирования можно проводить и вместе внутри одного процесса. Наиболее полным и популярным является тестирование в несколько этапов. Сначала система тестируется «в тёмную» (*Black box*), а потом уже — с максимально известными данными (*White box*). В таком случае результаты тестирования будут наиболее полными.

Также в случае сочетания различных методов используются разные подходы к тестированию: снаружи и изнутри, внешнего или внутреннего нарушителя, но всегда с отсутствием намеренных деструктивных шагов в отношении тестируемой инфраструктуры.

**Модель атак на системы**

Теперь посмотрим на то, как к вопросу взлома относятся *Black hat*.

Современные атаки на системы — это целый комплекс мероприятий, в результате чего взлом и заражение сети не происходят «вдруг из ничего». Этому предшествует целый набор действий. Модель *Cyber-Kill Chain* и её расширенная версия описывают все этапы атаки.

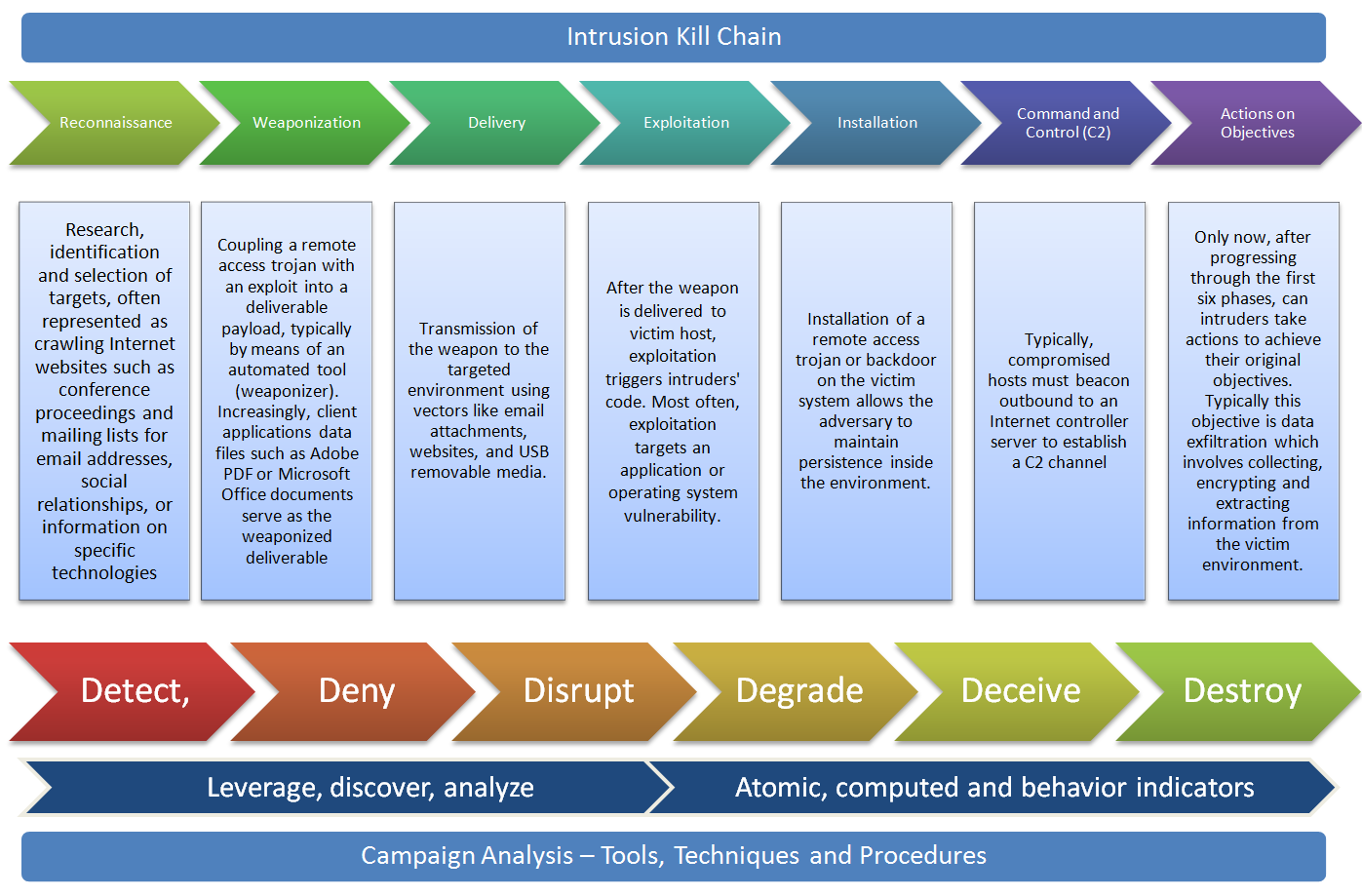
[](https://lms-cdn.skillfactory.ru/assets/courseware/v1/8d7944fbb8768d38b5ebefeb6b8b2357/asset-v1:SKILLFACTORY+hack_pentest+2020+type@asset+block/image5.png)

Рисунок 7. Структура модели Cyber-Kill Chain. Источник: [wordpress.com](https://countuponsecurity.files.wordpress.com/2014/08/killchain.png)

И другая вариация этой же модели, более наглядная:

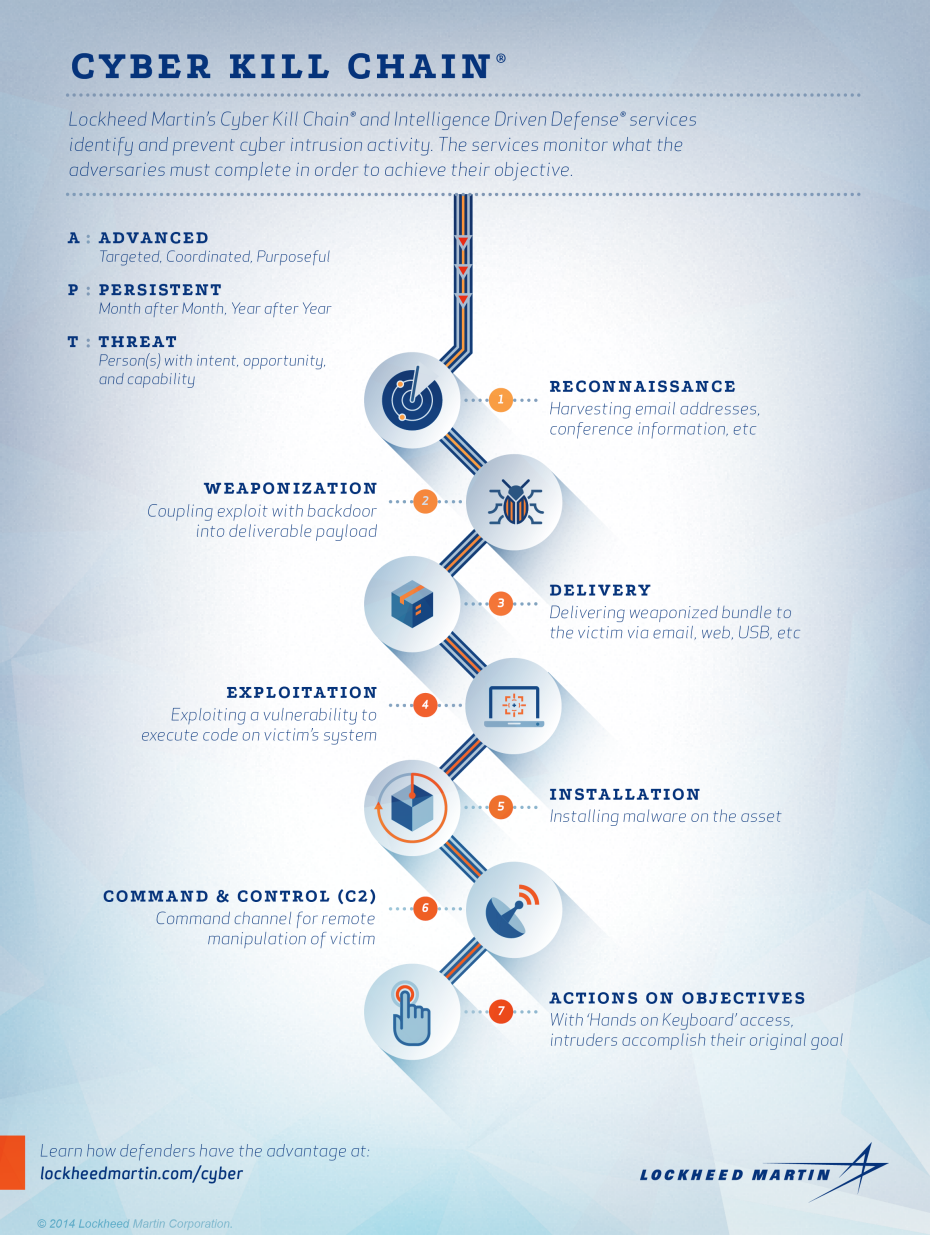


Рисунок 8. Структура модели Cyber-Kill Chain. Источник: [blogspot.com](https://3.bp.blogspot.com/-C9xaaAVSMD0/WA9nuQd7RgI/AAAAAAAAGq0/hGXHERwRQhQwrpm9XPHWqB3mOPzPeWplwCLcB/s1600/killchain.png)

Модель *Cyber-Kill Chain* делится на 7 этапов:

* 1. **Разведка**: исследование, идентификация и выбор целевой системы для взлома.
  2. **Вооружение**: написание или оснащение софтом для совершения нападения.
  3. **Доставка**: донесение вредоносного контента до целевой системы.
  4. **Заражение**: запуск вредоносного кода или эксплуатация уязвимости системы.
  5. **Инсталляция**: открытие удалённого доступа и другие действия с заражённой системой.
  6. **Получение управления**: управление заражённой системой.
  7. **Выполнение действий**: сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.

В целом, эту модель можно использовать для того, чтобы проектировать систему защиты и вырабатывать меры противодействия нападению. Более подробно с моделью можно ознакомиться в [статье на Хабре](https://habr.com/ru/company/panda/blog/327488/), в [статье на SecurityLab](https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/325123.php) или в [первоисточнике](https://csrc.nist.gov/CSRC/media/Presentations/The-Cyber-OODA-Loop-How-Your-Attacker-Should-Help/images-media/day3_security-automation_930-1020.pdf) (спойлер: там сложно, но возможно!).

Модель достаточно старая и теоретическая, но представляет собой систематический процесс достижения нарушителем цели для получения результата. С целью систематизации и моделирования угроз её и включают в практику служб ИБ.

**Базовая методология пентеста**

Теперь перейдём к базовой методологии пентеста. Она реализуется в 5 этапах:

* 1. **Сбор информации** (*Recon*) — поиск данных об организации и сотрудниках в открытых источниках, социальных сетях, на форумах и блогах.
  2. **Поиск технической базы** (*Mapping* или *Enumeration*) — определение существующих ресурсов, приложений и используемых технических средств в организации.
  3. **Анализ уязвимостей и угроз** (*Discovery* или *Vulnerability* *Analysis*) — обнаружение уязвимостей в системах безопасности и приложениях с применением набора инструментов и утилит, как коммерческих, так и разработанных непосредственно в компании пентестеров.
  4. **Эксплуатация** (*Exploitation*) — имитация реальной кибератаки, опираясь на ранее полученные данные об уязвимостях с дальнейшим анализом.
  5. **Формирование отчёта** (*Reporting*) — оформление результатов выполненного пентеста с предложениями по улучшению существующей системы безопасности.

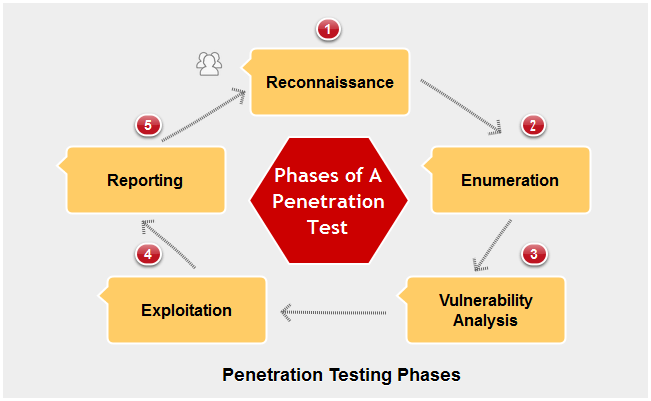


Рисунок 9. Этапы базовой методологии пентеста. Источник: [techbeamers.com](https://cdn.techbeamers.com/wp-content/uploads/2017/05/Penetration-Testing-Life-Cycle-5-Phases.png)

В зависимости от вкладываемого смысла и преследуемых целей данная модель может содержать 4-8 (можно придумать и больше) этапов или фаз. С основными этапами и применяемыми инструментами мы будем работать на практике в ходе курса.

Помимо базовой модели тестирования, существует несколько различных документированных методик оценки, связанных с тестированием на проникновение. Преимущество применения стандартов в том, что они позволяют проводить тестирование последовательно и опираясь на стандартизированные приёмы.

**Задание 1.3.1**

1/1 point (graded)

Расставьте этапы базовой методологии пентеста по порядку.

Введите ответ в окне ниже:

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**   Дополнительные материалы о методологии**

* + [Руководство по методологии тестирования безопасности](https://www.isecom.org/research.html#content5-9d) с открытым исходным кодом (*OSSTMM*).
  + [Открытый проект безопасности веб-приложений (OWASP)](https://owasp.org/www-project-top-ten/).
  + [Стандарт выполнения испытаний на проникновение (PTES)](http://www.pentest-standard.org/index.php/Main_Page).
  + [База знаний MITRE ATT&CK](https://attack.mitre.org/) (не совсем методика).
  + [Information System Security Assessment Framework (ISSAF)](http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf).

**Задание 1.3.2**

1/1 point (graded)

Какая угроза для веб-приложений по *OWASP Top 10* не является критической?

Уязвимость *XXE*

Уязвимость *XSS*

*DDoS*

Некорректная настройка параметров безопасности

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Подведём итог**

При проведении пентеста специалисты могут использовать несколько методологий (даже, как правило, используют несколько), стремятся к тому, чтобы охватить весь спектр возможных угроз организации. При этом учитываются технические, организационные и правовые риски: пентестер исключает деструктивные действия, которые наносят ущерб организации. От действий хакера пентест отличается в первую очередь тем, что тестировщик полностью контролирует уровень воздействия на инфраструктуру организации.

**Задание 1.3.3**

1/1 point (graded)

Какой этап не входит в модель *Cyber Kill Chain*?

*Delivery*

*Installation*

*Recognize*

*BGP*

*Backdoor*

*Reconnaissance*

*Explotation*

верно

Ответ

Верно:

*Recognize* — отношения к *CKC*-модели не имеет

*BG*P — протокол динамической маршрутизации

*Backdoor* — троян, отношение к пентесту имеет, к модели *CKC* — только как составляющая этапа, а не основной этап

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Задание 1.3.4**

1/1 point (graded)

Что подразумевается под аббревиатурой *EDGAR* по методике *PTE*S?

Имена разработчиков стандарта

*Electronic Data Gathering, Analysis, and Retrieval system*

Название робота-пылесоса

*Exploitation Destructive Gathering And Request*

верно

Ответ

Верно:

*EDGAR* — система электронного сбора, анализа и поиска данных. Осуществляет автоматический сбор, проверку, индексацию, приём и передачу представлений компаниями и другими лицами, которые по закону обязаны подавать формы в Комиссию по ценным бумагам и биржам США.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Ваш вопрос по теме юнита**

0 points possible (ungraded)

*Напишите вопрос в поле ниже:*

Code Editor



1

нет вопросов

Чтобы выйти, нажмите ESC и затем TAB или щёлкните вне редактора кода.

верно

верно

При проведении тестирования на проникновение важно учитывать юридические аспекты, а именно выполнение работ в соответствии с договором и соблюдение УК РФ.

Статьи УК РФ:

* [272](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) — неправомерный доступ к компьютерной информации.
* [273](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) — создание, использование и распространение вредоносных компьютерных программ.
* [274](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/) — нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Эти статьи УК РФ чётко описывают нам то, что нельзя делать с информацией, в том числе, что нельзя создавать и распространять вредоносные приложения (бэкдоры, трояны и т.д.). Безусловно, преступления в сфере компьютерной информации регламентируются не только указанными выше статьями, но и множеством федеральных законов, приказами ФСТЭК, ФСБ, стандартами Банка России.

В данном случае указаны статьи из УК РФ как самые широко применяемые. Если кратко, то ответственность за совершённые действия в сфере компьютерной информации наступает в следующих случаях:

1. Хакер получил доступ к охраняемой законом информации либо воспользовался вредоносной программой.
2. При этом его поймали с поличным и/или имеются доказательства, что это именно он (что происходит крайне редко).
3. Доказан преступный умысел либо халатность.



Рисунок 1. Американский хакер Кевин Митник. Источник: [ferra.ru](https://www.ferra.ru/thumb/1600x0/filters:quality(75):no_upscale()/imgs/2019/03/17/21/2955593/ea113dce1102077be36e9e9d5839518c86263aff.jpg)

При проведении тестирования на проникновение действия пентестера направлены в сторону эксплуатации максимально возможного количества уязвимостей. При этом возможно наступление события, когда пентестер неосознанно (случайно, непреднамеренно) получит доступ к информации разного уровня конфиденциальности.

С другой стороны, получение несанкционированного доступа к конкретной информации может быть одной из задач проведения тестирования на проникновение (кроме случая с банковской тайной).

Есть также законы, предусматривающие наказание за неправомерный доступ к критической информации (ФЗ-187) и персональным данным (ФЗ-152).

Таким образом, все действия, связанные с проведением тестирования на проникновения «снаружи», должны быть строго регламентированы договором.

**Задание 1.4.1**

1/1 point (graded)

В каких случаях при работе с информационными системами наступает уголовная ответственность?

В случае получения доступа к банковской тайне

В случае кражи аккаунта в социальной сети

В случае многоадресной почтовой рассылки с вредоносным вложением

В случае размещения фотографий коллег с корпоратива у себя в соцсети

В случае цитирования К. Маркса в публичном поле

верно

Ответ

Верно:

273, 272 статьи УК РФ и закон 395-1 о банковской тайне.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

В случае выполнения работ с иностранным подрядчиком нужно учитывать специфику законодательства той страны, резидентом которой является заказчик.

**Европа**

В вопросах тестирования на проникновение европейские страны регламентируют ответственность по-разному, объединяет всех только *GDPR* или [Общий регламент защиты персональных данных](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D0%BE_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), и он, безусловно, не в полной мере описывает все компьютерные преступления.

**США**

Основной закон США о компьютерных преступлениях действует с 1986 года — «О мошенничестве и злоупотреблениях, связанных с компьютерами» — и сейчас включён в Свод законов США. Кроме федерального законодательства США, касающегося компьютерных преступлений и безопасности, действует множество законов внутри каждого отдельного штата.

**ОСНОВНЫЕ ДОКУМЕНТЫ ДЛЯ ПРОВЕДЕНИЯ ПЕНТЕСТА**

Таким образом, чтобы минимизировать риски при выполнении работ, необходимо составить и подписать с заказчиком следующие документы (или их аналоги):

1. Договор о проведении пентеста (*Pentest agreement*).
2. Договор о неразглашении *NDA* (*Non-Disclosure agreement*, аналог в РФ — Соглашение о конфиденциальности).
3. Договор об отказе от претензий (*Cancellation agreement*).

**ОСОБЕННОСТИ СТАНДАРТА PCI DSS**

Требования к тестированию на проникновение в индустрии платёжных карт ([PCI DSS](https://ru.wikipedia.org/wiki/PCI_DSS)) регламентируются стандартом по защите информации. Он не намного отличается от обычного тестирования, проводимого с использованием методик *OSSTMM* и *OWASP*. Стандартом *PCI DSS* рекомендуется придерживаться правил *OWASP* при проведении как пентеста, так и аудита, но, тем не менее, отличия есть.

Основные отличия тестирования по *PCI DSS* от тестирования на проникновение в широком смысле этого слова заключаются в следующем:

* + Стандартом не регламентируется (а значит, и не требуется) проведение атак с использованием социальной инженерии.
  + Все проводимые проверки должны максимально минимизировать угрозу «Отказа в обслуживании» (*DoS*). Следовательно, проводимое тестирование должно осуществляться методом «серого ящика» с обязательным предупреждением администраторов соответствующих систем.
  + Основная цель такого тестирования — это попытка осуществления несанкционированного доступа к данным платёжных карт (*PAN*, *Cardholder Name* и т.п.).

**Задание 1.4.2**

1/1 point (graded)

В чём заключается тестирование методом *Gray box*?

Тестирование ведётся вслепую, знаем только название организации, сайт, адрес

Тестирование ведётся с использованием учётной записи в системе, но без привилегий

Тестирование ведётся, используя доступ администратора и его привилегии

верно

Ответ

Верно:

*Gray box* — тестирование с частичными знаниями о системе (учётная запись пользователя без привилегий, знания об информационных системах и др.)

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

Под методом «серого ящика» (*Gray box*) подразумевается выполнение различного рода проверок с предварительным получением дополнительной информации об исследуемой системе на разных этапах тестирования. Это позволяет снизить риск отказа в обслуживании при проведении подобных работ в отношении информационных ресурсов, функционирующих в режиме 24/7.

В общем случае тестирование на проникновение по требованиям *PCI DSS* должно удовлетворять следующим критериям:

* + Анализ защищённости беспроводных сетей.
  + Сканирование информационной сети на наличие уязвимостей (*AsV*).
  + Проведение проверок на сетевом уровне (*Network-layer penetration tests*).
  + Проведение проверок на уровне приложений (*Application-layer penetration tests*).

С актуальной версией стандарта (на английском языке) *PCI DSS* вы можете ознакомиться по [ссылке](https://lms-cdn.skillfactory.ru/assets/courseware/v1/a5257dad02f84c1d0755d7d3915f7f9d/asset-v1:SKILLFACTORY+hack_pentest+2020+type@asset+block/PCI-DSS-v4_0.pdf).

Это основные моменты, которые касаются проведения пентеста в отношении юридических лиц и владельцев информационных систем.

**ЗАЩИТА ИНФОРМАЦИИ ЧАСТНЫХ ЛИЦ И ПРАВО НА ЗАБВЕНИЕ**

Информацию частных лиц в РФ защищает ФЗ-152 «Закон о персональных данных», и в нём есть (как и в общемировой практике) интерпретация «Права на забвение». Любое частное лицо, воспользовавшись этим правом, может удалять о себе информацию из обработки (из поисковой выдачи или форума, к примеру). Подробнее почитать о праве на забвение можно в [статье](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE_%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B1%D0%B2%D0%B5%D0%BD%D0%B8%D0%B5#%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F).

Если говорить упрощённо, то любой гражданин может потребовать (на определённых основаниях: недостоверные сведения, неактуальные сведения, сведения, распространяемые с нарушением законодательства Российской Федерации (порочащие честь и достоинство, например)) удаления информации о себе из интернета. Для этого достаточно заполнить форму на сайте и дождаться ответа.

Формы «Забвения» для примера:

* + [Яндекс](https://yandex.ru/support/abuse/troubleshooting/oblivion.html).
  + [Google](https://support.google.com/legal/troubleshooter/1114905#ts=1115655%2C6034194%2C6322223).
  + [Mail.ru](https://go.mail.ru/support/oblivion/).

Сфера проведения тестирования на проникновение регламентируется законодательством, и во избежание ответственности необходимо об этом помнить. В том числе и в ходе обучения: не ломать соседский *Wi-Fi*, не угонять чужой ящик и т.д.

Для получения и навыков в пентесте, и их совершенствования стоит использовать специальные площадки в интернете или собственные стенды.

**Задание 1.4.3**

1/1 point (graded)

Какие юридические документы (или их аналоги) для проведения тестирования на проникновение необходимо иметь на руках пентестеру перед началом работы?

Договор о проведении пентеста

Договор о неразглашении *NDA*

Договор об отказе от претензий

Всё вышеперечисленное

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Задание 1.4.4**

1/1 point (graded)

Может ли Василий Артемов воспользоваться правом на забвение и удалить о себе информацию с фотографией с гостевой книги, в которую он писал с десяток лет назад?

Да, ведь информация о нём, размещённая в интернете, ему не нравится

Да, в случае, если эта информация является неактуальной, потерявшей значение, недостоверной или распространяемой с нарушением закона

Да, если договориться с владельцем ресурса, на котором размещены данные

верно

Ответ

Верно:

Может воспользоваться в случае судебного решения, подтверждающего, что эта информация является неактуальной, потерявшей значение, недостоверной или распространяемой с нарушением закона.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

**Ваш вопрос по теме юнита**

0 points possible (ungraded)

*Напишите вопрос в поле ниже:*

Code Editor



1

нету вопросов

Чтобы выйти, нажмите ESC и затем TAB или щёлкните вне редактора кода.

верно

верно

Инструментарий, используемый для проведения пентеста, многообразен. А ещё он множится за счёт самописного ПО и сотен различных фреймворков/сборок и скриптов, но всё начинается с выбора операционной системы как основы машины для пентеста.

Такой выбор в разы меньше и, как правило, все дистрибутивы основаны на ядре Linux. Есть сборки и на ОС Windows, но их крайне мало (например, [PentestBox](https://pentestbox.org/)). ОС Linux позволяет максимально раскрыть возможности оборудования и гибко использовать ПО. Поэтому мы в курсе будем работать именно на нём.

Рассмотрим обзорно наиболее популярные дистрибутивы ОС.

## Kali Linux

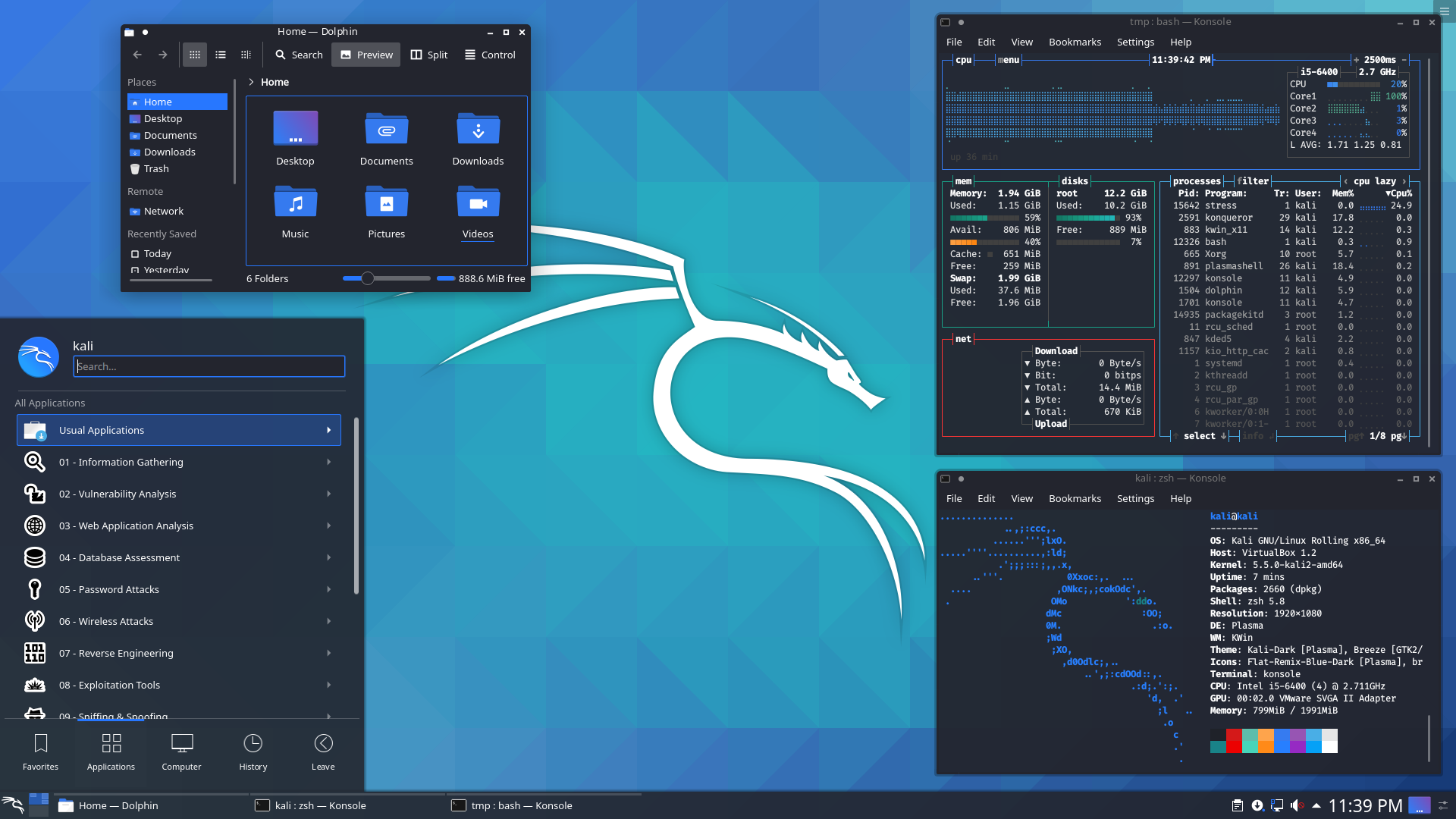
[](https://lms-cdn.skillfactory.ru/assets/courseware/v1/27ad62cceb6bfb8214c2dd5ccd2fce87/asset-v1:SKILLFACTORY+hack_pentest+2020+type@asset+block/release-2020.2-kali-kde-dark.png)

Рисунок 1. Интерфейс Kali Linux

На сегодняшний день это самая популярная операционная система и для пентестеров, и для хакеров, и для простых специалистов по информационной безопасности. Разрабатывается и поддерживается Offensive Security Ltd., и корнями уходит к ранее популярному дистрибутиву для тестирования безопасности BackTrack. BackTrack имел специальный криминалистический режим, который по наследству перешёл и в Kali, что позволяет использовать её для проведения криминалистической работы.

Kali включает одну из самых полных подборок инструментов для специалистов в области компьютерной безопасности: от средств для тестирования веб-приложений и проникновения в беспроводные сети до программ для считывания данных с идентификационных RFID-чипов. В комплект входит коллекция эксплоитов и более 300 специализированных утилит для проверки безопасности, таких как Aircrack, Maltego, SAINT, Kismet, Bluebugger, Btcrack, Btscanner, Nmap, p0f. Мы поговорим о них и поработаем с ними в ходе курса.

Помимо этого, в дистрибутив включены средства для ускорения подбора паролей (Multihash CUDA Brute Forcer) и WPA-ключей (Pyrit) через задействование технологий CUDA и AMD Stream, позволяющих использовать GPU видеокарт NVIDIA и AMD для выполнения вычислительных операций.

Почитать про неё можно [здесь](https://ru.wikipedia.org/wiki/Kali_Linux) или на [официальном сайте](https://www.kali.org/), и там же скачать образ.

## Parrot Security OS

[](https://lms-cdn.skillfactory.ru/assets/courseware/v1/589041258c1704be1a4430f07294eac2/asset-v1:SKILLFACTORY+hack_pentest+2020+type@asset+block/image15.png)

Рисунок 2. Интерфейс Parrot Security OS. Источник: [hackware.ru](https://hackware.ru/wp-content/uploads/2019/01/menu-full.jpg)

Parrot Security OS является GNU/LINUX-дистрибутивом, основанным на Debian. Этот дистрибутив, как и Kali, позволяет полноценно проводить тестирование на проникновение, поиск, эксплуатацию и оценку уязвимостей, компьютерную криминалистику и анонимный сёрфинг. Он был разработан Frozenbox’s Team.

В отличие от других подобных операционных систем, Parrot OS является довольно облегчённым Linux-дистрибутивом и может работать на машинах с 256 МБ ОЗУ, он также подходит как для 32bit (i386), так и для 64bit (amd64).

Некоторые специальные выпуски работают на 32bit-машинах (486). Одной из особенностей дистрибутива является его готовность «из коробки» к анонимности, режим Anon Surf. В нём уже предустановлены некоторые средства анонимизации, а именно — при выборе Anonsurf Start весь трафик системы будет перенаправлен через сеть TOR. В том же разделе есть возможность использовать DNS-серверы проекта OpenNIC — это вненациональная альтернатива реестрам доменов верхнего уровня. Также предустановлено огромное количество утилит для проведения тестирования, как и в OS Kali (различия по наполнению есть!).

Подробнее об этом можно прочитать [здесь](https://ru.wikipedia.org/wiki/Parrot_Security_OS) и на [официальном сайте](https://www.parrotsec.org/).

## BackBox OS

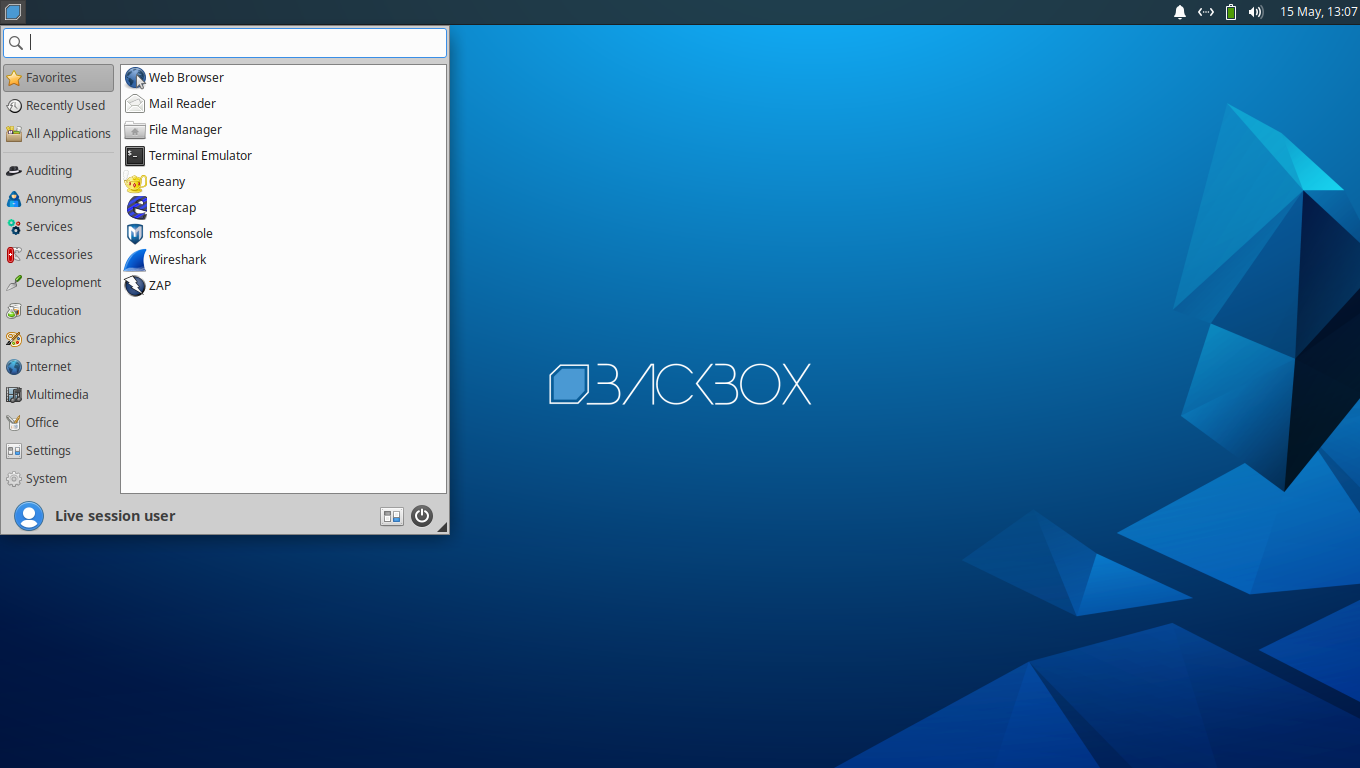


Рисунок 3. Интерфейс BackBox OS. Источник: [distrowatch.com](https://distrowatch.com/images/ktyxqzobhgijab/backbox.png)

BackBox OS — легковесный дистрибутив, основанный на Ubuntu.

В нём нет такого количества разнообразных инструментов, утилит и фреймворков, доступных прямо «из коробки», как, например, в Kali Linux или Parrot Security OS. Но ввиду использования оболочки XFCE BackBox Linux может отлично подойти и для повседневного использования на личном компьютере (в отличии от тех же Kali Linux и Parrot Security OS).

Как и в остальных операционных системах для специалистов по информационной безопасности, содержит «из коробки» режим Anonymous mode, при его использовании весь системный трафик пропускается через TOR-прокси. В этом режиме отрабатывают скрипты для смены MAC-адреса системы и Hostname, также при выключении режима все временные файлы удаляются с помощью интегрированного пакета BleachBit.

## BlackArch Linux

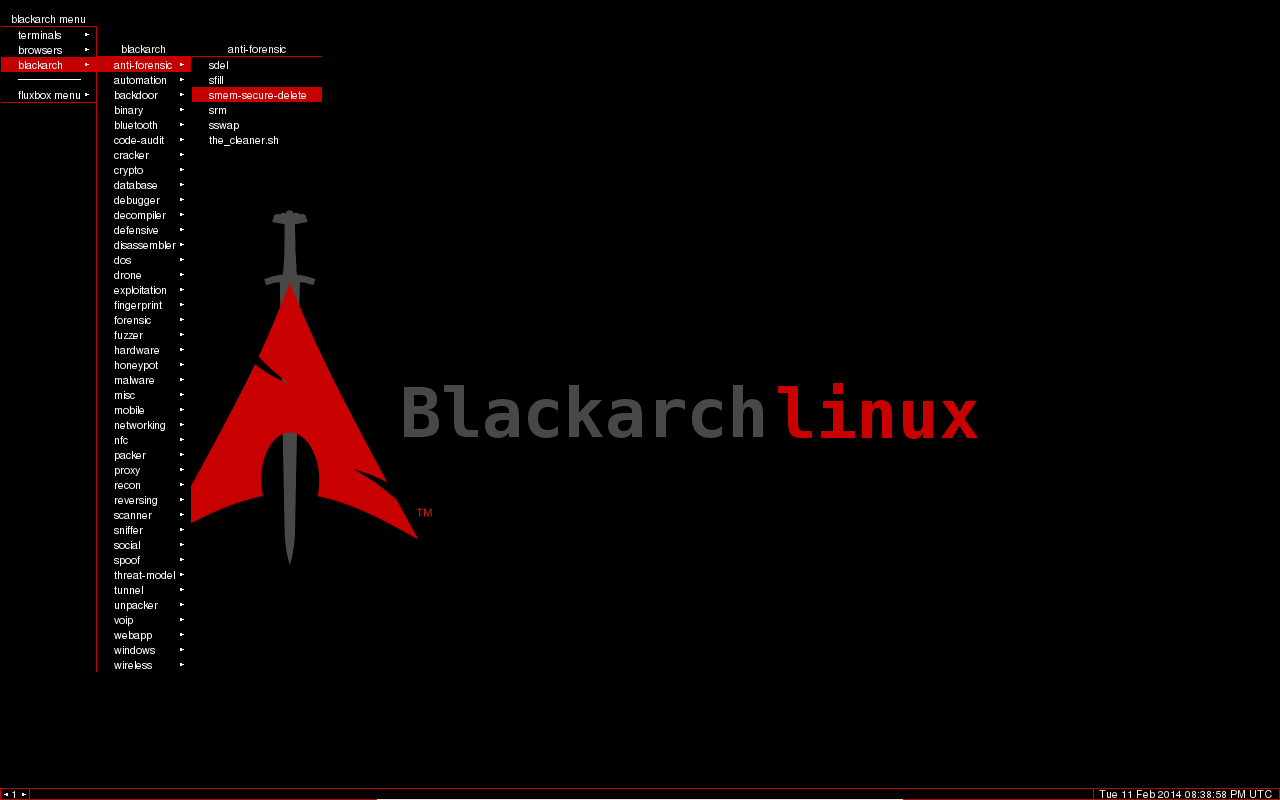
[](https://lms-cdn.skillfactory.ru/assets/courseware/v1/6e07118b4d8eb472d92720f8a24bc262/asset-v1:SKILLFACTORY+hack_pentest+2020+type@asset+block/image12.png)

Рисунок 4. Интерфейс BlackArch Linux. Источник: [zenway.ru](https://zenway.ru/uploads/02_14/blackarchlinux_004.png)

BlackArch Linux — это дистрибутив для тестирования на проникновения и, как предыдущие дистрибутивы, предлагает огромное количество возможного ПО для проведения тестирования: в его арсенале есть более 2000 различных инструментов и утилит, которые можно доустанавливать по мере необходимости. Основан он на Arch Linux и отличается от собратьев тем, что дружественность к пользователю не является приоритетом, и плохо подойдёт для повседневной работы.

Подробнее об этом можно прочитать [здесь](https://ru.wikipedia.org/wiki/BlackArch) или на [официальной странице](https://blackarch.org/) .

## Сканеры портов, уязвимостей

Помимо операционной системы, при проведении пентеста, естественно, нужны дополнительные инструменты. На начальном этапе основными из них являются **сетевые сканеры**. Сканирование проводится с целью обнаружения живых хостов в сканируемой сети, открытых портов на хостах, версий сервисов, работающих на этих портах, с целью дальнейшего выявления уязвимостей.

**Уязвимость** — слабое место узла, которое может быть использовано для реализации атаки. Уязвимостью может быть не только ошибка в программном коде, но и просто неправильная конфигурация сервиса.

Утилит для сканирования существует большое количество и, как правило, они подбираются и используются в зависимости от задач, возлагаемых на сканирование, технических возможностей (пропускная способность канала, наличие файрволов, средств обнаружения вторжений и т.д.). Наиболее популярные бесплатные сетевые сканеры: nmap, Zmap (nmap с графической оболочкой), masscan и многие другие.

Существуют коммерческие продукты, отличающиеся возможностями и ориентированностью на удобство пользователя: XSpider, Nessus (бесплатен для некоммерческого использования), Nexpose и другие.

Помимо локальных инструментов для проведения сканирования, существуют и онлайн-поисковики, которые периодически сканируют интернет и хранят результаты сканирования: [Shodan](https://www.shodan.io/), [Censys](https://censys.io/).

На первом этапе изучения тестируемой системы всегда нужно сходить в поисковик и посмотреть, что им уже было найдено и, соответственно, сразу получить какие-то данные.

Более подробно об этом можно прочитать [здесь](https://www.securitylab.ru/blog/company/pt/349200.php).

## Веб-прокси или комбайны для тестирования веб-приложений

Для тестирования веб-приложений используются перехватывающие приложения, позволяющие инспектировать и модифицировать трафик между атакующей рабочей станцией и тестируемым веб-приложением. Наиболее популярными являются [Burp Suite](https://portswigger.net/) и [Zed Attack Proxy](https://www.zaproxy.org/).

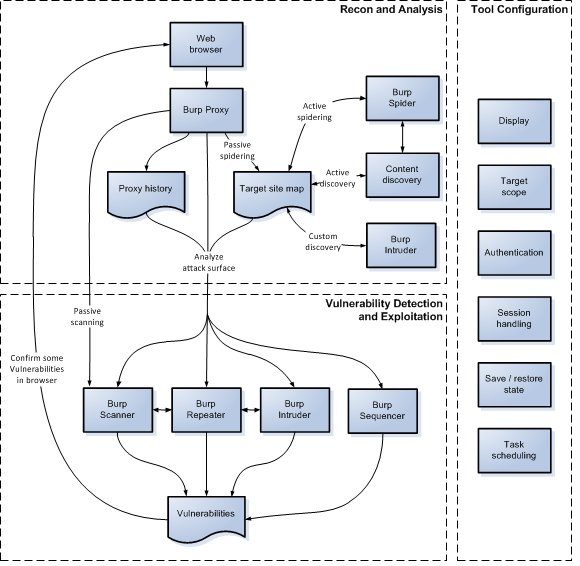


Рисунок 5. Совокупность инструментов Burp Suite. Источник: [hsto.org](https://hsto.org/getpro/habr/post_images/910/c12/d43/910c12d43eab95f4bb29834efcd7e584.png)

Они позволяют производить сканирование веб-приложений для автоматизированного выявления ряда типов уязвимостей, инспектировать и модифицировать трафик, манипулировать с запросами и их повторной отправкой, а также для выполнения пользовательских атак для поиска и эксплуатации нестандартных уязвимостей.

Все тестирования веб-приложений производятся с применением Burp Suite (в 95%), и без его инструментов и функционала производить пентест будет затруднительно и займёт гораздо больше времени.

## Подведём итог

В течение курса мы соберём свой стенд на базе операционной системы, предназначенной для аудита и тестирования на проникновение, разберёмся с разным инструментарием и научимся работать со сканерами безопасности и перехватывающими прокси.

### Задание 1.5.1

1/1 point (graded)

Какую группу инструментов пентестер использует в самом начале работы над тестированием системы? верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Задание 1.5.2

1/1 point (graded)

#### Расставьте процессы сбора информации при тестировании системы на проникновение по порядку:

верно

Ответ

Верно:

В начале любого тестирования на проникновение ведётся сбор данных о тестируемой системе, и начинать надо с общедоступных поисковиков (Google, Bing и т.д.), затем — специализированные поисковики (Censys и т.д.), и только потом уже переходить к активной фазе сканирования. Это мы обсудим, когда будем изучать OSINT.

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Параметры вашего компьютера

0 points possible (ungraded)

*Напишите параметры компьютера, который вы будете использовать для обучения (CPU, Memory, HDD, видеокарта, Wi-Fi). Какой дистрибутив ОС вы бы хотели использовать?*

Code Editor



1

Intel Core i7-7500U CPU @ 2.70 GHZ, 2901 МГц, ядер 2, логических процессоров- 4

2

RAM- 8.00 ГБ

3

Локальный диск С - 445 ГБ

4

AMD Radeon R7 M340

5

Wireless IAP, Wireless IAP v2

6

Хотел бы испльзовать Kali Linux

Чтобы выйти, нажмите ESC и затем TAB или щёлкните вне редактора кода.

верно

верно

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Ваш вопрос по теме юнита

0 points possible (ungraded)

*Напишите вопрос в поле ниже:*

Code Editor



1

нет вопросов

Чтобы выйти, нажмите ESC и затем TAB или щёлкните вне редактора кода.

верно

верно

В настоящее время обучение и сертификация специалистов по информационной безопасности стали востребованными. Как правило, на международном рынке их спрашивает работодатель при трудоустройстве и заказчик при заключении договора на проведение пентеста. Сейчас в сфере пентеста наиболее популярна сертификация от **Offensive Security** (от разработчиков *Kali Linux*). Всего ими разработано порядка семи курсов (включая бесплатный тренинг по *Kali Linux*):

* + *OSCP (Offensive Security Certified Professional)*,
  + *OSCE (Offensive Security Certified Expert)* ,
  + *OSWE (Offensive Security Web Expert)* ,
  + *OSWP (Offensive Security Wireless Professional)* ,
  + *OSEE (Offensive Security Exploitation Expert)* ,
  + *MSFU (Metasploit Unleashed)*.

Все курсы охватывают разные направления пентеста и предполагают итоговый экзамен.

Обучение и сдача экзаменов являются достаточно сложными, и проходят под лозунгом разработчиков курса «*try harder*» ввиду того, что для успешной сдачи требуется широкий набор навыков и умений, но при этом обеспечивается минимальная поддержка обучающегося (она всё же есть, и в большинстве случаев заключается во фразе «*try harder*»).

Ранее была очень популярна и распространена сертификация от *EC-Council*, более знакомая специалистам в области тестирования на проникновения как *CEH (Certified Ethical Hacker)*. Фактически популярность сертификата *CEH* сравнима с *OSCP*, тем не менее, среди специалистов в области тестирования на проникновение звание *OSCP* зачастую ценится выше, нежели *CEH* — это связано в первую очередь с тем, что *CEH* в большей степени ориентирован на теоретические знания соискателя (например, до недавнего времени для прохождения был доступен только тест с выбором варианта ответов), в то время как *OSCP* направлен на проверку практических навыков.

И несмотря на то, что *EC-Council* теперь тоже предлагают практические экзамены — *CEH (Certified Ethical Hacker), ECSA (EC-Council Certified Security Analyst) и LPT (Licensed Penetration Tester)*— аналогичные сертификаты от *Offensive Security* ценятся выше, вероятно, из-за сложности тестовых заданий.

Сертификаций в сфере информационной безопасности (не только пентеста) огромное количество, и ознакомиться с ними можно в интерактивной [карте курсов](https://pauljerimy.com/security-certification-roadmap/).

**Задание 1.6.1**

1/1 point (graded)

В какой области карты международных сертификаций в сфере ИБ представлены сертификации по пентесту? верно

Ответ

Верно:

В этой карте собраны сертификации и обучения для всех направлений информационной безопасности, и стоит обратить внимание, что Penetration Testing курсы — это вторая справа колонка по ссылке выше

Some problems have options such as save, reset, hints, or show answer. These options follow the Submit button.