

# HackWare.ru

Этичный хакинг и тестирование на проникновение, информационная безопасность

## **Перевод официальной документации по Kali Linux: Общее использование (разное, всё остальное, после установки)**

### **Оглавление**

- 1. Введение (что такое Kali Linux и какие особенности у Kali)**
- 2. Установка (установка Kali Linux на настольные компьютеры и ноутбуки с использованием файлов «.ISO»)**
- 3. Виртуализация (виртуальные машины — Vmware, VirtualBox, Hyper-V и Vagrant)**
- 4. USB (портативная Kali на USB-накопителе)**
- 5. Кали на ARM (всё об устройствах ARM)**
- 6. Контейнеры (Docker и LXC/LXD)**
- 7. WSL (подсистема Windows для Linux)**
- 8. Облако (AWS, Azure и Linode)**
- 9. Документация Kali NetHunter (Kali на вашем телефоне Android)**
- 10. Общее использование (разное, всё остальное, после установки)**
  - 10.1 Метапакеты Kali Linux

10.2 sudo в Kali Linux

10.3 Вопросы и ответы по Xfce в Kali Linux

10.4 Переход на Python 3

10.5 Использование Python 2 в Kali

10.6 Исправление DPI (разрешающая способность): крупные шрифты

10.7 Отображение HiDPI (много точек на дюйм): всё мелкое

10.8 Режим Forensics (судебной экспертизы, IT криминалистики) в Kali Linux

10.9 Как установить драйверы для видеокарты NVIDIA

10.10 Branch (ветки) Kali

10.11 Настройка Yubikeys для аутентификации SSH

10.12 Программы, которые ведут себя иначе без прав root

10.13 Настройка RDP с Xfce

10.14 Кали в браузере (Guacamole)

10.15 Kali в браузере (noVNC)

10.16 Домены Kali

10.17 Сетевые репозитории Kali (/etc/apt/sources.list)

10.18 Kali Training

10.19 Переключение среды рабочего стола

10.20 Обновление Kali

## **11. Инструменты (инструменты внутри Kali)**

## 12. Решение проблем (когда что-то идёт не так)

---

В этом разделе собраны советы и подсказки по использованию Kali Linux, не попавшие в другие разделы.

### Метапакеты Kali Linux

Метапакеты используются для одновременной установки множества пакетов, которые перечислены как список зависимостей. Kali Linux использует их несколькими способами. Один из способов — позволить пользователям решать, сколько пакетов из общего списка Kali они хотели бы установить. Нужно установить пакеты только для работы самой Linux? Хотите пакеты, которых будет достаточно для выполнения пентеста в определённой области? Возможно, вы хотите установить все пакеты, которые имеются в Kali? В любой из этих задач вам помогут метапакеты.

Подробности по использованию смотрите в отдельной статье «[Метапакеты Kali Linux](#)».

### sudo в Kali Linux

В версии 2020.1 Kali отказалась от использования root в качестве пользователя по умолчанию. Это означает, что для root не установлен пароль, и учётная запись, созданная во время установки, является единственной для использования. Можно установить пароль пользователя root и использовать эту учётную данную, но это не рекомендуется.

**sudo** — это способ доступа к инструментам, портам или службам, которым требуются административные привилегии. Поскольку sudo является мощным средством и может предоставить полный доступ к системе, не рекомендуется бездумно использовать sudo для каждой команды.

Поскольку Kali по умолчанию создаёт пользователя с правами

администратора, пользователи могут сразу же использовать sudo и указать свой пароль для аутентификации. Если пользователь хочет сделать так, чтобы при использовании sudo не запрашивался пароль, то это можно сделать, хотя это представляет угрозу безопасности. Если кто-то получит доступ к учётной записи пользователя, то он получит полный контроль над системой, даже не зная пароль администратора.

Чтобы включить использование sudo без пароля, выполните команду:

```
1 sudo apt install -y kali-grant-root && sudo dpkg-reconfigure kali-grant-root
```

Предыдущая команда устанавливает пакет, который позволит добавить пользователя в доверенную группу, которой не нужно будет указывать пароль при использовании sudo. Однако это не означает, что учётная запись root будет активирована.

Пример использования:

```
1
2
3 ls /root
4
5 ls: невозможно открыть каталог '/root': Отказано в доступе
6
7 sudo ls /root
8 [sudo] пароль для kali:
9 hello
10
11 sudo apt install -y kali-grant-root && sudo dpkg-reconfigure kali-grant-root
12
13 ...ТИПИЧНЫЙ ВЫВОД...
14
15 sudo ls /root
16 hello
17
```

Материалы по теме:

- [Что такое sudo](#)
- [Как пользоваться sudo](#)

## Вопросы и ответы по Xfce в Kali Linux

Новый рабочий стол Kali Linux невероятно быстр и великолепен. Вот несколько советов и приёмов, которые помогут вам быстро сориентироваться.

### Смена среды рабочего стола

**В:** Как из GNOME перейти на Xfce без переустановки Kali Linux?

**О:** Выполните команду:

```
1 sudo apt update && sudo apt install kali-desktop-xfce
```

Когда вас попросят выбрать «Диспетчер отображения по умолчанию», выберите **lightdm**.

Затем запустите

```
1 update-alternatives --config x-session-manager
```

и выберите параметр Xfce. Если вы также хотите удалить оконный менеджер Gnome, что мы не рекомендуем, пока вы не уверены на 100% что хотите перейти на Xfce, то запустите

```
1 apt purge --autoremove kali-desktop-gnome
```

Последнюю команду запускайте только после того, как уже выполните настройку Xfce.

В следующий раз, когда вы войдёте в систему после перезагрузки, у вас будет окружение рабочего стола Xfce. Если вы не запускали команду **update-alternatives**, вы можете выбрать «**Xfce**» в селекторе

сеансов в верхнем правом углу экрана входа в систему.

**В:** Я установил Xfce, но он не похож на превью. Как мне заставить его выглядеть так же?

**О:** Если у вас возникли проблемы, возможно, файл конфигурации настроен неправильно. Сначала сделайте резервную копию папок **.cache**, **.config** и **.local**. Затем запуск

```
1 rm -r .cache .config .local
```

с последующей перезагрузкой, скорее всего, решит эти проблемы.

**В:** Как я могу получить образ Kali Linux с GNOME вместо Xfce?

**О:** Просто загрузите образ Kali GNOME с  
<https://www.kali.org/downloads/>

**В:** Я пробовал Xfce, и мне он очень нравится, но я всё же хотел бы вернуться на GNOME. Как я могу это сделать?

**О:** Для установки GNOME выполните команду:

```
1 sudo apt update && sudo apt install kali-desktop-gnome
```

В следующий раз, когда вы войдёте в систему, вы можете выбрать «GNOME» в селекторе сеансов в верхнем правом углу экрана входа.

## HiDPI

**В:** У меня экран HiDPI, и все выглядит крошечным. Есть ли способ это исправить?

**О:** Смотрите страницу HiDPI.

## Снимки экрана

**В:** Как делать скриншоты?

**О:** Нажмите кнопку **Print Screen** на клавиатуре и будет сделан снимок экрана. В качестве альтернативы вы можете щёлкнуть значок Kazam на панели быстрого запуска (крайний правый значок на панели рядом с меню приложения) и выбрать «Снимок экрана».

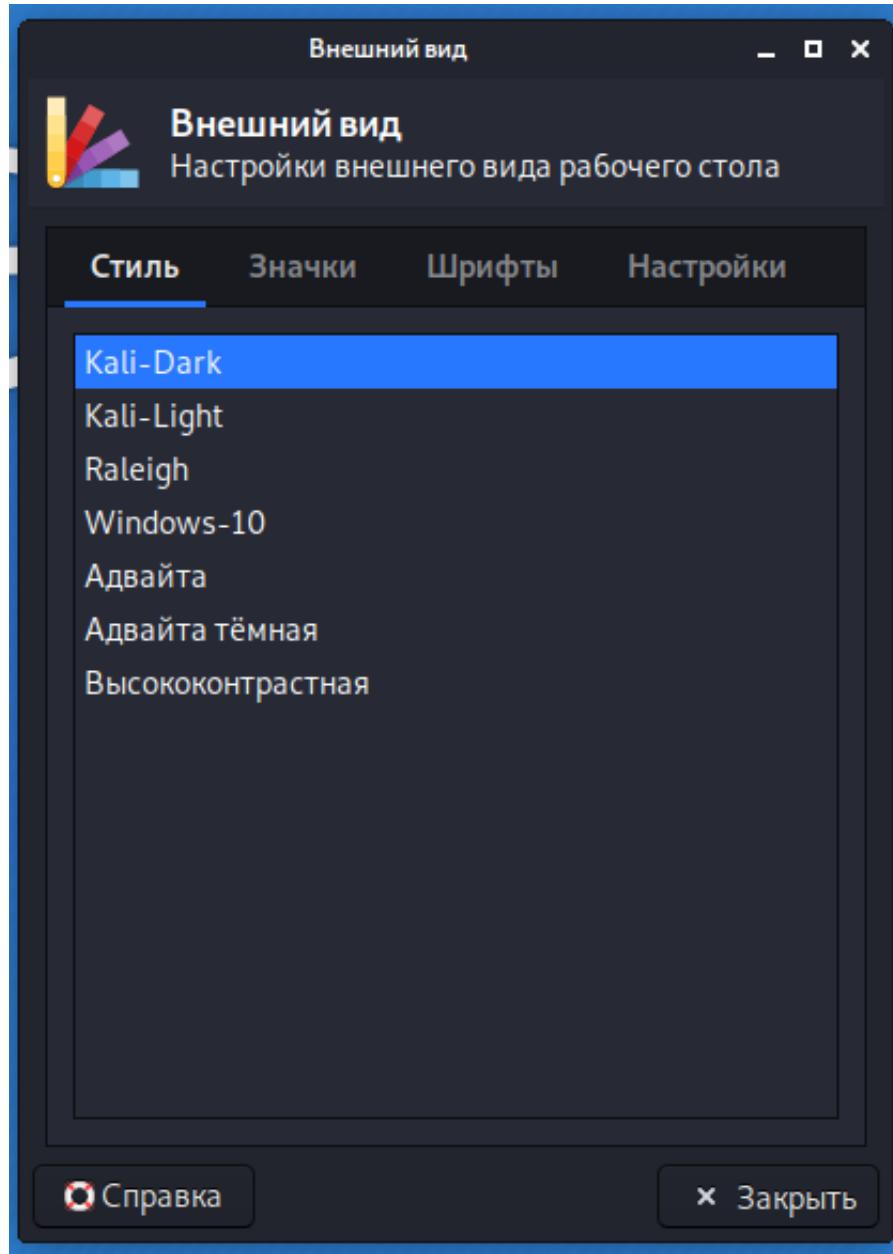
**В:** Как я могу записывать видео с действиями на экране?

**О:** Щёлкните значок Kazam на панели быстрого запуска (крайний правый значок на панели рядом с меню приложения) и выберите «Запись экрана».

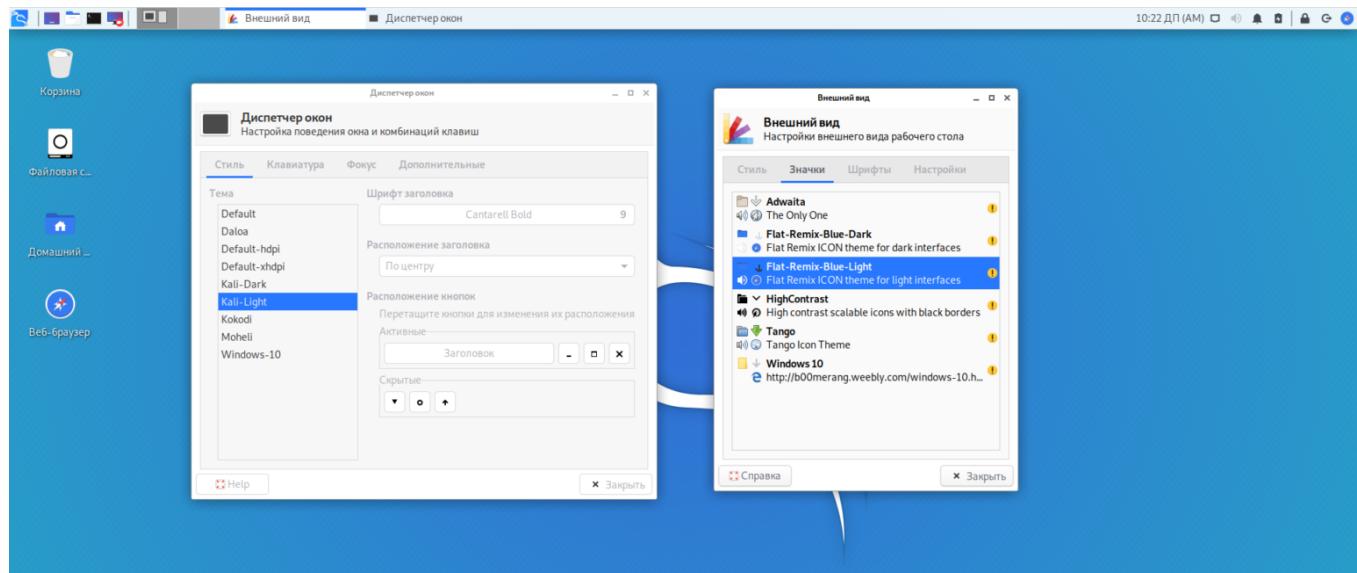
## Тема оформления

**В:** Как переключиться на более светлую или более тёмную тему?

**О:** Kali Linux предоставляет две темы по умолчанию: тёмную и светлую. Для переключения на светлую тему, перейдите в «Настройки» → «Внешний вид» и на вкладке «Стиль» выберите «Kali-Light». А на вкладке «Значки» выберите «Flat-Remix-Blue-Light».



Затем перейдите в «Настройки» → «Диспетчер окон» и на вкладке «Стиль» выберите «Kali-Light».



Для переключения со Светлой на Тёмную тему просто выберите **Dark** темы в этих же настройках.

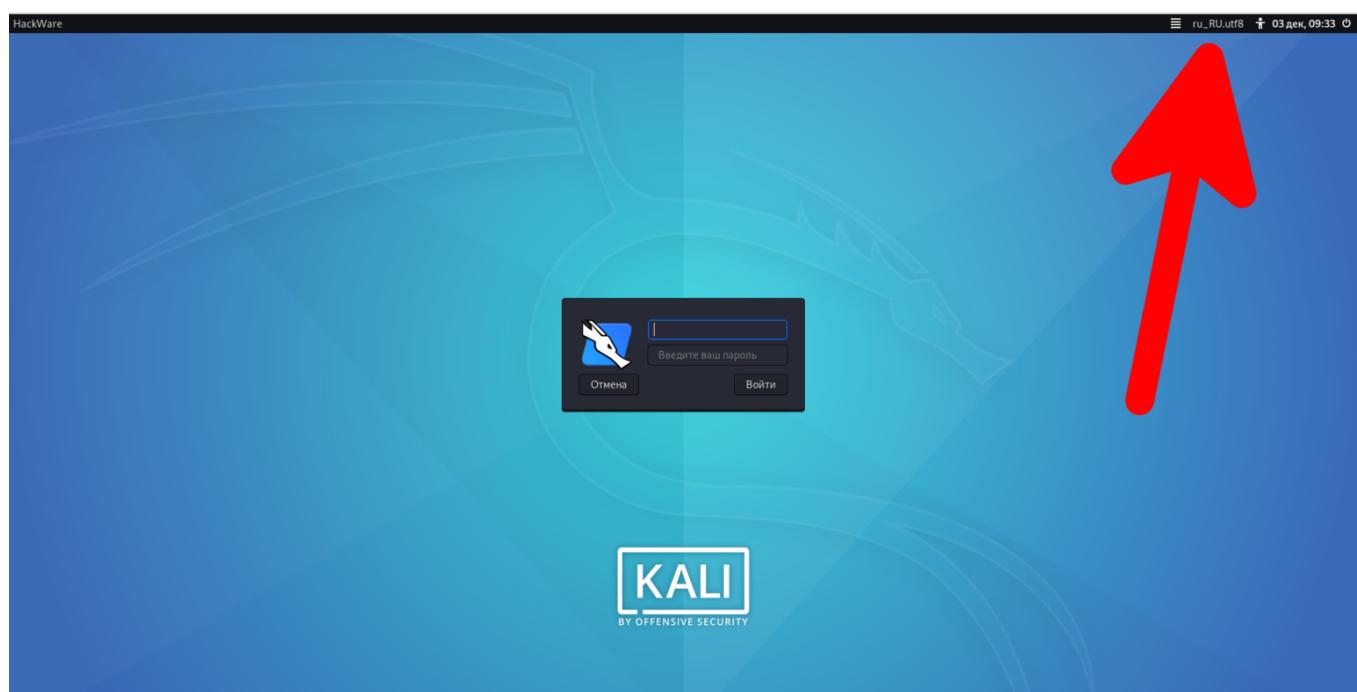
**В:** Мне нравятся кнопки на правой стороне, но ещё больше они мне нравятся на левой. Как я могу переключиться?

**О:** Вы можете перемещать кнопки с одной стороны на другую в **«Настройки → Диспетчер окон → Стиль → Расположение кнопок»**. Просто перетащите их на другую сторону от слова **«Заголовок»**.

## Языковые настройки

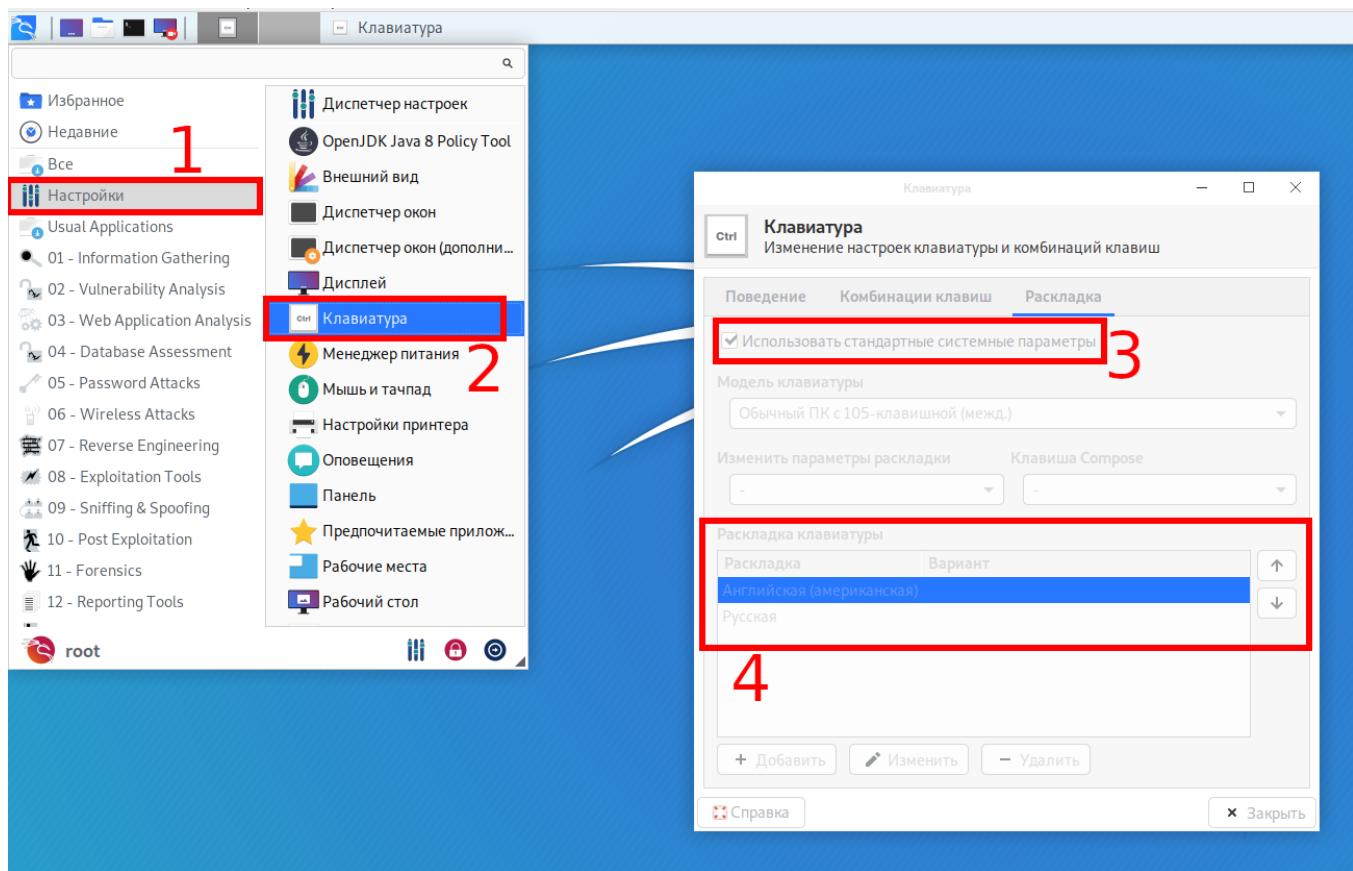
**В.** Как изменить язык Kali Linux?

**О:** В экране входа LightDM выберите желаемый язык в правой части верхней панели.



**В:** Как поменять раскладку клавиатуры?

**О:** Перейдите в **Настройки → Клавиатура → Раскладка**:



Чтобы выполнить настройку, снимите галочку с «**Использовать стандартные системные параметры**», в результате вы сможете добавить новые раскладки клавиатуры, выбрать раскладку клавиатуры по умолчанию, изменить комбинацию клавиш для смены клавиатуры.

Для изменения и установки других комбинаций клавиатуры, смотрите соседнюю вкладку «**Комбинация клавиш**».

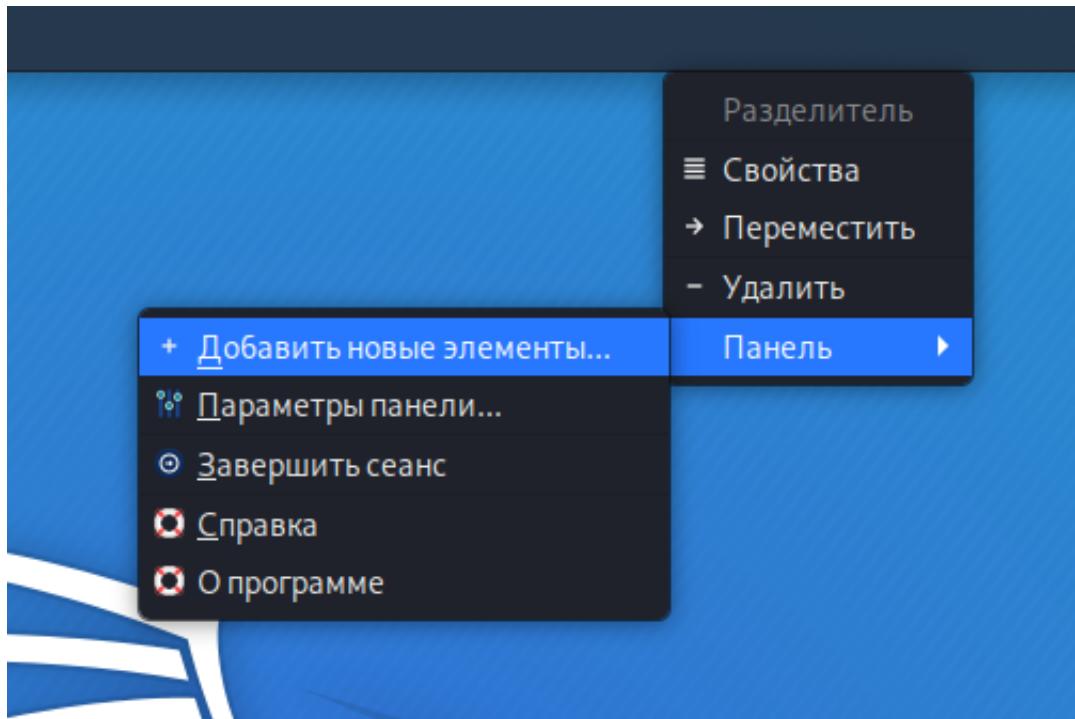
**В:** Как включить отображение языковой панели в верхнем меню Kali Linux

**О:** В Kali Linux отсутствует индикатор раскладки клавиатуры, то есть не показывается язык, который в данный момент выбран для ввода.

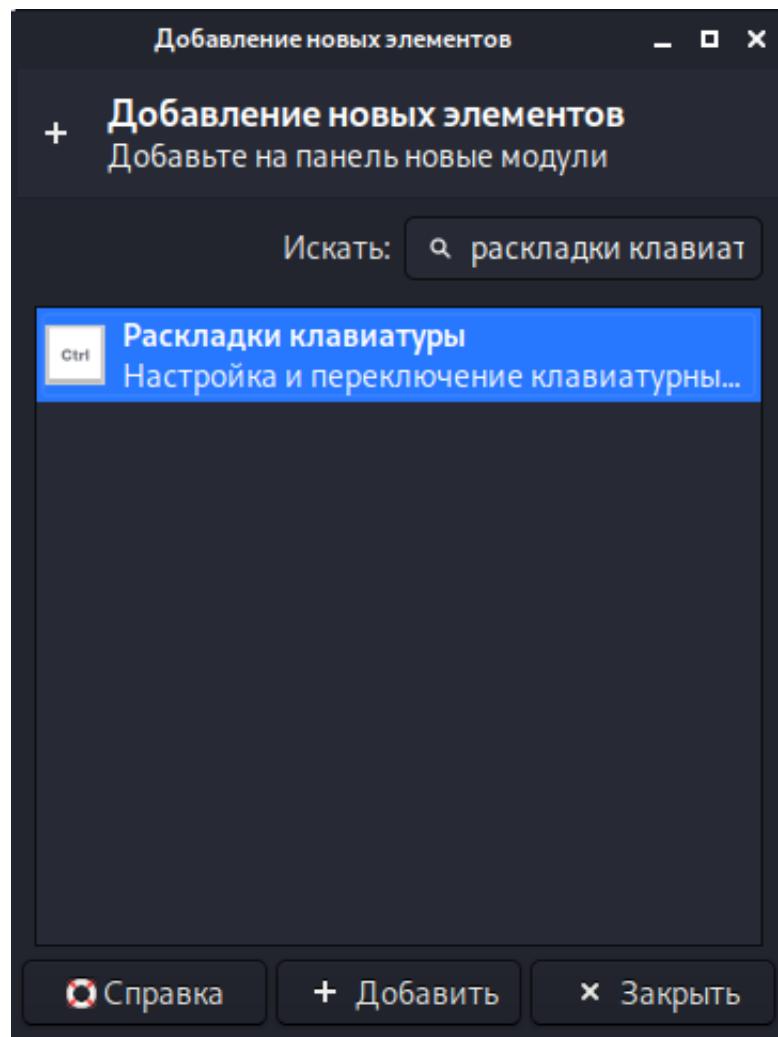
Для отображение языковой панели в виде кнопки с флагом, при клике по которому будет переключаться раскладка клавиатуры, сделайте следующее:

1. Кликните по верхней панели правой кнопкой мыши и выберите в открывшемся контекстном меню **Панель → Добавить**

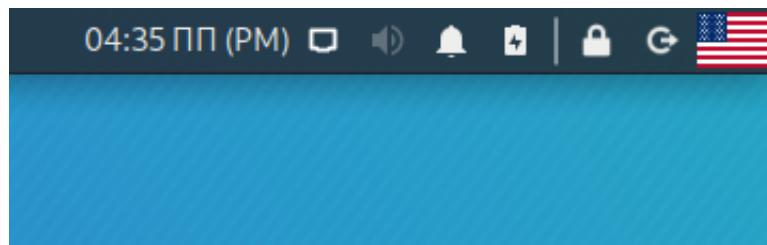
## **НОВЫЕ ЭЛЕМЕНТЫ:**



2. Найдите «раскладки клавиатуры» и нажмите кнопку «Добавить»:



После этого появится языковая панель в виде флага:



## Переход на Python 3

Kali Linux полностью перешла на Python 3. Это означает, что любой инструмент, присутствующий в репозиториях Kali, который использовал Python 2, был либо удалён, либо конвертирован для использования в Python 3. Во всех этих инструментах в качестве шебанга указан **/usr/bin/python3**.

Что касается пакетов, которые поступают прямо из Debian, они сделали то же самое для большинства пакетов, но есть несколько исключений, когда пакетам разрешено продолжать полагаться на Python 2. Однако эти пакеты были обновлены, поэтому все эти скрипты используют **/usr/bin/python2** в качестве их шебанга, то есть в них использование **python2** указано явно (вместо прежнего **python**).

Благодаря этим изменениям Debian больше не нужно предоставлять **/usr/bin/python**, а недавние обновления эффективно избавятся от этой символической ссылки.

К сожалению, когда вы загружаете скрипт Python в Интернет, он, скорее всего, будет иметь **/usr/bin/python** в качестве его шебанга. Если вы попытаетесь выполнить его, не исправляя строку shebang, вы получите ошибку, подобную этой:

```
1 zsh: /home/kali/test.py: bad interpreter: /usr/bin/python: no such
file or directory
```

То есть плохой интерпретатор **/usr/bin/python**, нет такого файла или каталога.

В Debian вы можете восстановить символьическую ссылку **/usr/bin/python**, установив один из пакетов:

- **python-is-python2**, если вы хотите, чтобы он указывал на python2
- **python-is-python3**, если вы хотите, чтобы он указывал на python3

## Сохранение обратной совместимости в Kali

Учитывая большое количество пользователей, которые не знали, как избежать вышеуказанной ошибки, было решено, что Kali будет продолжать поставлять Python 2 по умолчанию (пока Debian всё ещё предоставляет его) и что **/usr/bin/python** будет указывать на него. Также сохранено несколько общих внешних модулей (например, **requests**), чтобы скрипты эксплойтов имели разумные шансы на успешное выполнение.

Однако **pip** для Python2 (он же **python-pip**) больше не используется, **/usr/bin/pip** совпадает с **/usr/bin/pip3**, и он установит модули для Python 3. Для получения дополнительной информации смотрите вопросы и ответы ниже.

Эта совместимость была реализована за счёт того, что **kali-linux-headless** рекомендовал **python2**, **python-is-python2** и **offsec-awaе-  
python2**, так что они устанавливаются по умолчанию и могут быть удалены пользователями, которые хотели бы избавиться от них.

Чтобы пользователи знали об этой ситуации, при входе в систему выводится сообщение:

```
1  ┌(Message from Kali developers)
2  |
3  | We have kept /usr/bin/python pointing to Python 2 for backwards
4  | compatibility. Learn how to change this and avoid this message:
|   => https://www.kali.org/docs/general-use/python3-transition/
```

```
5 |  
6 | L(Run "touch ~/.hushlogin" to hide this message)  
7 |
```

```
root@HackWare-Kali: ~  
Файл Действия Правка Вид Справка  
└─(mial@HackWare-Kali)-[~]  
$ sudo su -  
(Message from Kali developers)  
We have kept /usr/bin/python pointing to Python 2 for backwards  
compatibility. Learn how to change this and avoid this message:  
⇒ https://www.kali.org/docs/general-use/python3-transition/  
└─(Run "touch ~/.hushlogin" to hide this message)  
└─(root@HackWare-Kali)-[~]  
#
```

В этом сообщении дана ссылка на страницу, перевод которой вы сейчас читаете. Ниже будет показано, что нужно сделать, чтобы это сообщение не выводилось.

## Часто задаваемые вопросы

**В:** Я загрузил скрипт Python, что мне делать?

**О:** Вам нужно осмотреть его шебанг. Стока shebang — это первая строка скрипта, которая начинается с символов **#!** за которыми следует путь к интерпретатору, который будет использоваться для выполнения скрипта.

Если интерпретатором является **/usr/bin/python**, вам следует прочитать документацию, чтобы узнать, может ли скрипт работать с Python 3. Если да, то вам следует обновить строку shebang, чтобы она указывала на **/usr/bin/python3**. В противном случае вам следует обновить его, чтобы она указывал на **/usr/bin/python2**.

Хорошие строки shebang, которые можно оставить как есть:

- **#!/usr/bin/python3**
- **#!/usr/bin/python2**
- **#!/usr/bin/env python3**
- **#!/usr/bin/env python2**

Плохие строки shebang, которые необходимо обновить:

- **#!/usr/bin/python**
- **#!/usr/bin/env python**

**В:** Как я могу избавиться от сообщения о Python 2 которое показывается при входе в систему?

**О:** Сообщение будет отображаться только до тех пор, пока **/usr/bin/python** указывает на устаревший Python 2. Теперь, когда вы знаете об этой ситуации и знаете, как исправить строку shebang в старых скриптах, вы можете безопасно избавиться от **/usr/bin/python**:

```
1 sudo apt remove python-is-python2
```

Или вы можете указать на Python 3:

```
1 sudo apt install python-is-python3
```

Любое из этих действий избавит от приведённого выше сообщения.

В качестве альтернативы, если вы хотите, чтобы **/usr/bin/python** указывал на python2, и вы всё равно хотите отключить это сообщение, вы можете сделать это:

```
1 mkdir -p ~/.local/share/kali-motd  
2 touch ~/.local/share/kali-motd/disable-old-python-warning
```

**В:** У меня есть скрипт Python 2, который не запускается, что мне делать?

**О:** Если ваш скрипт Python 2 использует модули, которых нет среди тех, которые поставляются в пакете совместимости **offsec-awaе-руеnв** (смотрите список [здесь](#)), то вы можете попробовать **руеnв** для установки полностью изолированной среды Python 2, где вы можете использовать **рір** для установки дополнительных модулей. Смотрите следующий раздел «Использование Python 2 в Kali».

**В:** Я хочу рір для Python 2, как я могу его вернуть?

**О:** Попробуйте **руеnв**. Смотрите следующий раздел «Использование Python 2 в Kali».

**В:** Я написал скрипт на Python, что мне делать?

**О:** Будьте вежливы с конечными пользователями:

- чётко задокументируйте, работает ли ваш код с Python 3 или Python 2
- используйте **/usr/bin/python3** или **/usr/bin/python2** в качестве строки shebang, она более выразительна, чем **/usr/bin/python**, и с большей вероятностью даст желаемый результат
- обновите его для совместимости с Python 3, если это ещё не так

## Использование Python 2 в Kali

Всё ещё существует довольно много востребованных инструментов, которые не были перенесены с Python 2 на Python 3, что вызывает проблемы при их использовании. Эта страница расскажет, как безопасно использовать устаревшую версию.

### руеnв

Python 2 больше не поддерживается в репозиториях Debian. Это означает, что мы должны найти способ обойти эту проблему. **руеnв** решает эту проблему, позволяя нам устанавливать несколько версий Python, которые не конфликтуют друг с другом. В настоящее время его нет в репозиториях Debian или Kali, поэтому нам нужно будет

установить его из исходников. К счастью, есть удобный [скрипт установки](#), выпущенный авторами. Давайте вместе пройдём установку и настройку.

Начнём с установки зависимостей:

```
1 sudo apt install -y build-essential libssl-dev zlib1g-dev libbz2-dev  
libreadline-dev libsqlite3-dev wget curl llvm libncurses5-dev  
libncursesw5-dev xz-utils tk-dev libffi-dev liblzma-dev python3-  
openssl git
```

Далее мы просто запустим скрипт установки, написанный на bash. Если ZSH является оболочкой по умолчанию, после этого нам придётся отредактировать файл **.zshrc**.

```
1 curl https://pyenv.run | bash
```

Если мы используем ZSH, то теперь мы добавим соответствующие строки в наш **.zshrc**.

```
1 echo 'export PYENV_ROOT="$HOME/.pyenv"' >> ~/.zshrc  
2 echo 'export PATH="$PYENV_ROOT/bin:$PATH"' >> ~/.zshrc  
3 echo -e 'if command -v pyenv 1>/dev/null 2>&1; then\n  eval "$(pyenv  
init -)"\nfi' >> ~/.zshrc
```

Продолжим настройку:

```
mial@HackWare-Kali:~
```

Файл Действия Правка Вид Справка

```
(mial@HackWare-Kali)-[~]
$ echo 'export PYENV_ROOT="$HOME/.pyenv"' >> ~/.zshrc

(mial@HackWare-Kali)-[~]
$ echo 'export PATH="$PYENV_ROOT/bin:$PATH"' >> ~/.zshrc

(mial@HackWare-Kali)-[~]
$ echo -e 'if command -v pyenv 1>/dev/null 2>&1; then\n    eval "$(pyenv init -)"\nfi' >> ~/.zshrc

(mial@HackWare-Kali)-[~]
$ exec $SHELL
(mial@HackWare-Kali)-[~]
$ pyenv
pyenv 1.2.22
Usage: pyenv <command> [<args>]

Some useful pyenv commands are:
activate      Activate virtual environment
commands      List all available pyenv commands
deactivate    Deactivate virtual environment
doctor        Verify pyenv installation and development tools to build pythons.
exec          Run an executable with the selected Python version
global        Set or show the global Python version(s)
help          Display help for a command
hooks         List hook scripts for a given pyenv command
init          Configure the shell environment for pyenv
install       Install a Python version using python-build
local         Set or show the local application-specific Python version(s)
prefix        Display prefix for a Python version
rehash        Rehash pyenv shims (run this after installing executables)
root          Display the root directory where versions and shims are kept
shell         Set or show the shell-specific Python version
shims         List existing pyenv shims
uninstall     Uninstall a specific Python version
--version     Display the version of pyenv
version       Show the current Python version(s) and its origin
version-file   Detect the file that sets the current pyenv version
version-name   Show the current Python version
version-origin Explain how the current Python version is set
versions      List all Python versions available to pyenv
virtualenv    Create a Python virtualenv using the pyenv-virtualenv plugin
virtualenv-delete Uninstall a specific Python virtualenv
virtualenv-init  Configure the shell environment for pyenv-virtualenv
virtualenv-prefix  Display real_prefix for a Python virtualenv version
virtualenvs    List all Python virtualenvs found in '$PYENV_ROOT/versions/*'.
 whence        List all Python versions that contain the given executable
 which        Display the full path to an executable

See `pyenv help <command>' for information on a specific command.
For full documentation, see: https://github.com/pyenv/pyenv#readme
```

(mial@HackWare-Kali)-[~]

Теперь мы можем установить Python 2 и сделать его нашей версией Python по умолчанию в **pyenv**:

- 1 pyenv install 2.7.18
- 2 pyenv global 2.7.18
- 3 pyenv versions
- 4 python

```
mial@HackWare-Kali:~\nФайл Действия Правка Вид Справка\n(mial@HackWare-Kali)-[~]\n$ pyenv install 2.7.18\nDownloading Python-2.7.18.tar.xz ...\n→ https://www.python.org/ftp/python/2.7.18/Python-2.7.18.tar.xz\nInstalling Python-2.7.18 ...\nInstalled Python-2.7.18 to /home/mial/.pyenv/versions/2.7.18\n\n(mial@HackWare-Kali)-[~]\n$ pyenv global 2.7.18\n\n(mial@HackWare-Kali)-[~]\n$ pyenv versions\nsystem\n* 2.7.18 (set by /home/mial/.pyenv/version)\n\n(mial@HackWare-Kali)-[~]\n$ python\nPython 2.7.18 (default, Jan 12 2021, 15:43:59)\n[GCC 10.2.1 20201224] on linux2\nType "help", "copyright", "credits" or "license" for more information.\n>>> \n
```

Теперь мы можем устанавливать зависимости по мере необходимости для любых инструментов, которые мы используем. Когда мы хотим вернуться к Python 3, нам просто нужно установить значение **global** на **system**.

1	pyenv global system
2	python -V

```
mial@HackWare-Kali:~\nФайл Действия Правка Вид Справка\n(mial@HackWare-Kali)-[~]\n$ pyenv global system\n\n(mial@HackWare-Kali)-[~]\n$ python -V\nPython 3.9.1\n\n(mial@HackWare-Kali)-[~]\n$ \n
```

Следует иметь в виду, что нужно устанавливать зависимости через **pip**. **apt** будет не очень любезен, если вы пытаетесь установить

зависимости Python 2 через него и через **pip**, поэтому в этом случае просто придерживайтесь **pip**.

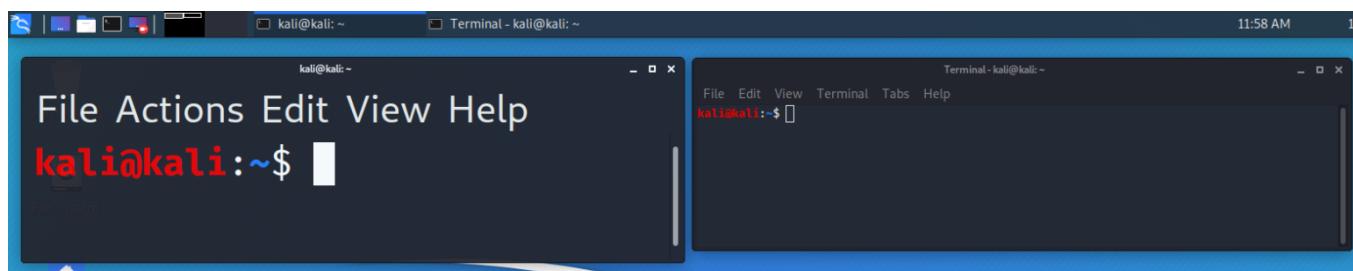
## Исправление DPI (разрешающая способность): крупные шрифты

После запуска Kali Linux некоторые вещи могут оказаться больше, чем ожидалось. Это может быть из-за неправильного DPI (точек на дюйм) / PPI (пикселей на дюйм). Если вещи выглядят меньше, чем ожидалось, вы можете посмотреть следующее руководство по HiDPI.

Это может происходить по разным причинам, например, проблемы могут вызывать драйвера графической карты и/или профиль монитора.

### Проблема

При открытии некоторых приложений шрифт может отображаться больше, чем ожидалось, как в примере ниже. Здесь вы можете увидеть два разных терминальных программного обеспечения: одно слева использует Qt (**QTerminal**), а другое справа использует GTK (**xfce4-terminal**).



Qt слишком велик, и его нужно изменить. Сначала нам нужно найти, какое значение нужно изменить, затем нам нужно применить это изменение.

### Локализация проблемы

Сначала мы используем [xrdb](#), который ищет в базе данных X-сервера, чтобы увидеть, какие значения там есть:

Вывод:

```
1 *customization: -color
2 xft.antialias: 1
3 xft.hinting: 1
4 xft.hintstyle: hintslight
5 xft.rgba: rgb
6 xcursor.theme_core: 1
```

Нет никаких признаков того, что DPI заранее определён. Пора переходить к следующему инструменту.

Используя [xdpyinfo](#), мы можем посмотреть отображаемую информацию о X, которая используется в настоящее время (поскольку всё будет определяться динамически в различных точках, например на странице входа, подключение нового экрана и т. д.):

```
1 xdpyinfo | grep 'dimensions\|resolution'
```

Вывод:

```
1 dimensions: 1680x1050 pixels (160x90 millimeters)
2 resolution: 267x296 dots per inch
```

Эти значения показаны только один раз, что означает, что есть только один монитор. Но размер обнаруживаемого физического экрана 160×90 мм, это является ключом, почему шрифт очень большой (поскольку DPI огромен). Мы также можем видеть, что разрешение экрана установлено на 1680×1050, а DPI составляет ~267.

Затем мы можем использовать [xrandr](#), поскольку она обрабатывает расширение RandR (изменение размера и поворот), чтобы увидеть, соответствует действительности ли то, что она сообщает:

```
1 xrandr -q | grep -iw 'screen\|connected'
```

Вывод:

```
1 Screen 0: minimum 8 x 8, current 1680 x 1050, maximum 32767 x 32767
2 HDMI-0 connected 1680x1050+0+0 (normal left inverted right x axis y
axis) 160mm x 90mm
```

Опять один экран. Кроме того, его разрешение совпадает с тем, что нам сообщил **xdisplayinfo**. Мы можем увидеть его с помощью кабеля HDMI, разрешение и размер такие же.

Проверяя логи X, мы видим:

```
1 grep DPI /var/log/Xorg.0.log
```

Вывод:

```
1 [      7.324] (--) NVIDIA(0): DPI set to (266, 296); computed from
"UseEdidDpi" X config
```

Это очень близко к значению DPI, о котором сообщил **xrandr** (но меньше на единицу). Мы видим, что используемая видеокарта — это NVIDIA, и она пытается получить значение DPI из EDID (графический процессор пытается прочитать данные с монитора)

При желании мы можем посмотреть значение EDID с помощью [edid-decode](#):

Устанавливаем пакет с программой:

```
1 sudo apt install -y edid-decode
```

Запускаем:

```
1 xrandr --props | edid-decode -c -s
```

Пример вывода:

```
1
2
3     EDID version: 1.3
4     ...SNIP...
5     Maximum image size: 16 cm x 9 cm
6     ...SNIP...
7     Warnings:
8     Block 0 (Base Block):
9         Basic Display Parameters & Features: Dubious maximum image size
10        (160x90 is smaller than 10x10 cm)
11        Failures:
12        All Blocks:
13        One or more of the timings is out of range of the Monitor Ranges:
14            Vertical Freq: 24 - 75 Hz (Monitor: 23 - 75 Hz)
15            Horizontal Freq: 27.000 - 79.976 kHz (Monitor: 26.000 - 68.000
16            kHz)
17            Maximum Clock: 148.500 MHz (Monitor: 150.000 MHz)
18        EDID conformity: FAIL
```

Похоже, что **значения EDID неверны**, поэтому нам не следует слушать монитор! Нам нужно будет вручную определить используемые значения.

Самый простой способ сделать это — посмотреть на марку/модель экрана (есть ли наклейка на задней/нижней части устройства?). В противном случае мы можем использовать старомодный метод и померить рулеткой.

**Почему значения оказались неправильными?**

Так какой же, по мнению ОС, размер нашего экрана?

Используя немного математики (1 см составляет 10 мм, а 25,4 мм — 1 дюйм), мы можем преобразовать миллиметры (мм) в дюймы (дюймы):

Помните, что на выходе были размеры: 1680×1050 пикселей (160×90 миллиметров), поэтому мы принимаем «ширину» как 160 и «высоту<sup>2</sup>» как 90.

```
1 echo 'print(160/25.4)' | python3
2 6.299212598425197
3 echo 'print(90/25.4)' | python3
4 3.543307086614173
5
```

Теперь мы можем найти размер диагонали экрана, выполнив  $\sqrt{(\text{ширина}^2 + \text{высота}^2)}$  = **диагональ**:

```
1 echo 'print( ((160/25.4) ** 2)+((90/25.4) ** 2) ) ** (0.5)' | python3
2 7.227385728616465
```

На наклейке на обратной стороне экрана указано, что он 20 дюймов, но обнаружено только 7,2 дюйма!

## Поиск правильного значения

Используя формулу  $\sqrt{(\text{ширина}^2 + \text{высота}^2)} / \text{диагональ} = \text{DPI}$ , получаем:

Помните, что на выходе были размеры: 1680×1050 пикселей (160×90 миллиметров), поэтому мы принимаем «ширину» как 1680 и «высоту» как 1050, а правильная диагональ — 20.

```
2 echo 'print( (((1680 ** 2)+(1050 ** 2) ) ** (0.5) ) / 20 )' | python3
3 99.05680188659434
4
```

Поэтому нам нужно установить DPI на 99×99, а не 267×296.

## Исправление проблемы

Есть несколько способов исправить это, каждый со своими плюсами и минусами:

- Редактирование **~/.Xresources** (рекомендуемый метод конфигурации X)
- Редактирование **~/.xsessionrc** (скрипт запуска X)
- Настройки драйвера NVIDIA
- Настройки графического интерфейса Xfce (конфигурация окружения рабочего стола)

## Xresources

Мы можем настроить X (для каждого пользователя). В окне терминала выполните следующие команды:

```
1
2 echo "Xft.dpi: 99" >> ~/.Xresources
3 cat ~/.Xresources
4 xft.dpi: 99
5 xrdb -merge ~/.Xresources
6
```

После запуска **xrdb -merge** выхода из системы не требуется, поэтому в следующий раз, когда вы откроете проблемную программу, шрифт теперь должен быть «нормальным».

## **xsessionrc**

Это скрипт оболочки, который автоматически запускается при графическом входе в систему. В окне терминала выполните следующие команды:

```
1
2 echo "xrandr --dpi 99" >> ~/.xsessionrc
3 cat ~/.xsessionrc
4 xrandr --dpi 99
5 xfce4-session-logout --logout
6
```

После выхода и повторного входа в следующий раз, когда вы откроете проблемную программу, шрифт теперь должен быть «нормальным».

## **Настройки драйвера NVIDIA**

Другой подход — заставить драйверы NVIDIA обрабатывать DPI.

Если для X нет файла конфигурации, мы собираемся его сгенерировать, а затем переместить:

```
1
2 sudo apt install -y nvidia-xconfig
3 sudo nvidia-xconfig
4 sudo mv /etc/X11/xorg.conf /usr/share/X11/xorg.conf.d/20-nvidia.conf
5
```

Теперь мы можем отредактировать файл конфигурации, включив следующие две строки в раздел «Устройство»:

```
1 Option "UseEdidDpi" "False"  
2 Option "DPI" "99 x 99"
```

Отредактируем файл:

```
1 sudo vim /usr/share/X11/xorg.conf.d/20-nvidia.conf
```

Изучим содержимое файла:

```
1  
2 cat /usr/share/X11/xorg.conf.d/20-nvidia.conf  
3 ...SNIP...  
4 Section "Device"  
5     Identifier      "Device0"  
6     Driver          "nvidia"  
7     VendorName     "NVIDIA Corporation"  
8     Option          "UseEdidDpi" "False"  
9     Option          "DPI" "99 x 99"  
10    EndSection  
11 ...SNIP...
```

Выйдем из сессии:

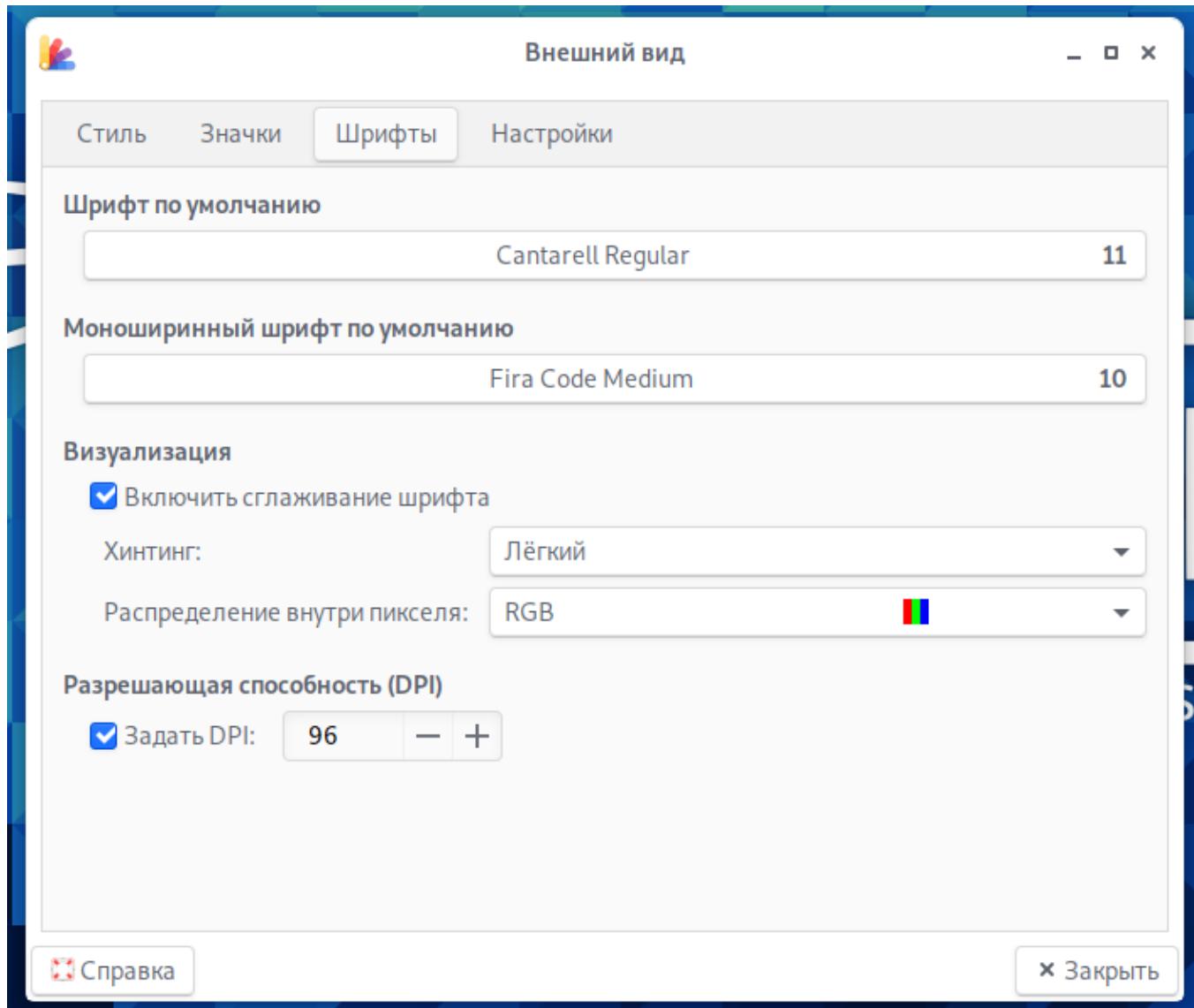
```
1 xfce4-session-logout --logout
```

После выхода и повторного входа в следующий раз, когда вы откроете проблемную программу, шрифт теперь должен быть «нормальным».

## Настройки Xfce

Мы можем настроить Xfce, перейдя в: **Kali → Настройки → Внешний вид → Шрифты → Разрешающая способность (DPI)**

Включите: «Задать DPI» и установите значение на 99



Выход из системы не требуется, поэтому в следующий раз, когда вы откроете проблемное программе, шрифт теперь должен быть «нормальным».

## Дополнительный материал

Ссылки на дополнительные материалы для чтения:

- <https://http.download.nvidia.com/XFree86/Linux-x86/390.132/README/dpi.html>
- <https://wiki.ubuntu.com/X/Troubleshooting/HugeFonts>
- <https://wiki.archlinux.org/index.php/HiDPI>
- <https://wiki.archlinux.org/index.php/Xrandr>

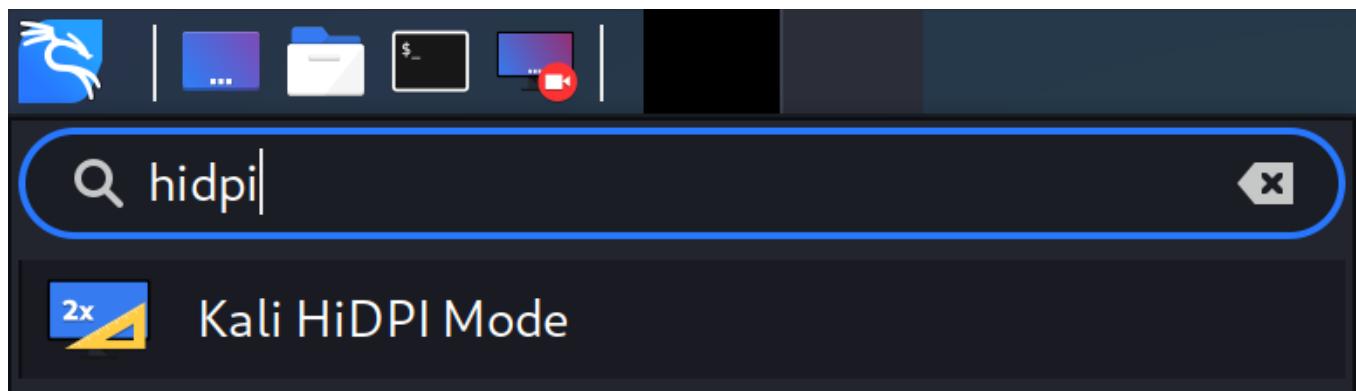
# Отображение HiDPI (много точек на дюйм): всё мелкое

После запуска Kali Linux некоторые элементы (окно/кнопки или текст/шрифт) могут отображаться меньшими, чем ожидалось. Это может быть из-за HiDPI (также известного как High DPI). Всё зависит от рассматриваемого программного обеспечения, от того, как оно было создано (например, GTK2, GTK3, Qt5 и т. д.). Это может произойти по разным причинам, например из-за драйверов графической карты и/или профиля монитора.

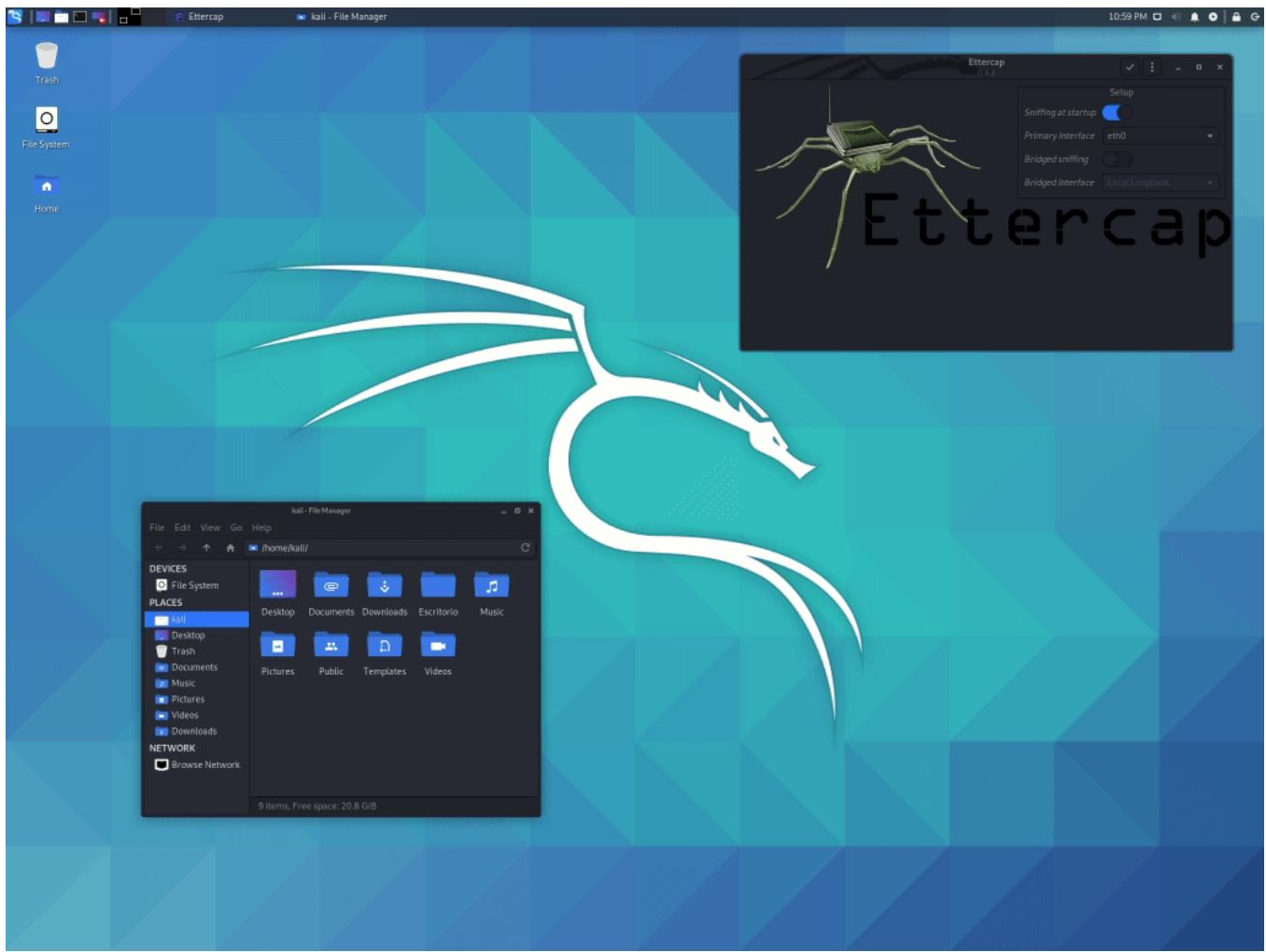
Если что-то выглядит больше, чем вы считаете «нормальным», ознакомьтесь с предыдущим руководством по исправлению DPI.

## Среды рабочего стола — Xfce

Xfce поддерживает мониторы HiDPI. Хотя вам может потребоваться изменить несколько настроек, в зависимости от вашего оборудования, версий и проблем, чтобы заставить его работать.



Чтобы упростить этот процесс, Kali теперь предоставляет режим HiDPI. Этот режим регулирует коэффициент масштабирования для интерфейсов на основе GTK, QT и даже Java, так что пользователю не нужно изменять каждый из них вручную. Вы можете переключить его, открыв «**Kali HiDPI Mode**» из меню приложений или запустив **kali-hidpi-mode** с терминала.



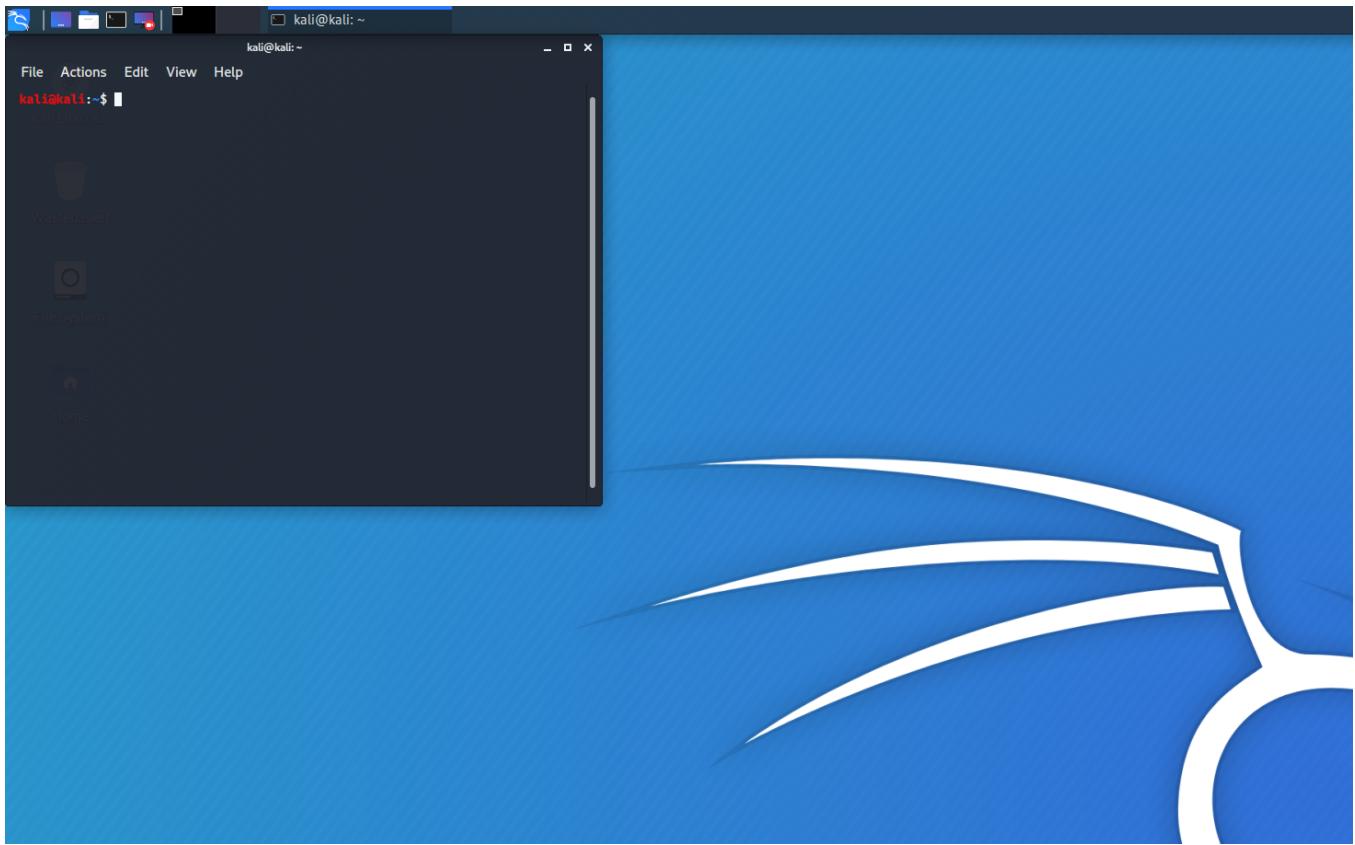
Несмотря на то, что **kali-hidpi-mode** может изменять коэффициент масштабирования без необходимости перезапуска, рекомендуется закрыть сеанс и снова войти в систему, чтобы убедиться, что все изменения применяются правильно.

Ниже приведено более подробное объяснение ручной настройки.

## Коэффициент масштабирования

### GTK

После входа в Kali обои могут выглядеть «нормально», но всё остальное может быть слишком мелким для чтения.

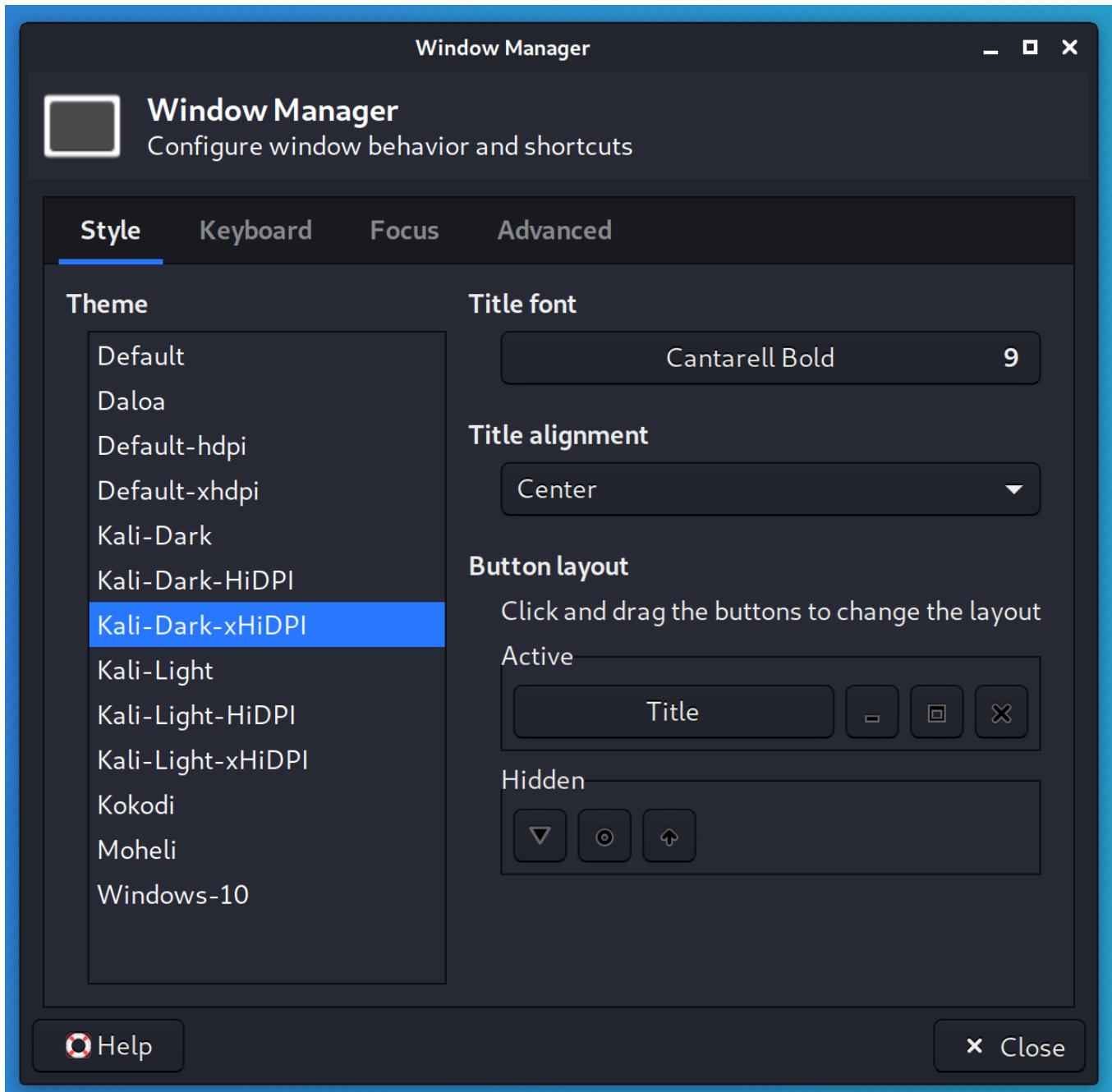


Увеличение «коэффициента масштабирования» с « $x_1$ » до « $x_2$ » должно решить эту проблему. У вас есть два способа сделать это: через командную строку или графический интерфейс:

- В окне терминала выполните следующие команды:

```
1
2 echo export GDK_SCALE=2 >> ~/.xsessionrc
3 xfconf-query -c xfwm4 -p /general/theme -s Kali-Dark-xHiDPI
4 xfconf-query -c xsettings -p /Gdk/WindowScalingFactor -n -t 'int' -s 2
5
```

- Графически:
- Меню Kali → Настройки → Внешний вид → Настройки → Масштабирование окон
- Меню Kali → Настройки → Внешний вид → Диспетчер окон → Тема: **Kali-Dark-xHiDPI**



Самый быстрый способ удалить все оставшиеся артефакты — выйти из системы и снова войти в неё.

## Qt

Некоторые приложения, такие как [qTerminal](#), не используют коэффициент масштабирования, описанный ранее, поэтому их нужно настраивать отдельно.

Для этого вам необходимо установить следующие переменные среды в файле `~/.xsessionrc`:

```
1 echo export QT_SCALE_FACTOR=2 >> ~/.xsessionrc
```

## Размер курсора

Включение настроек HiDPI может вызвать некоторые проблемы с размером мыши, и вы можете увидеть, как его размер меняется в зависимости от приложения, в которое вы его поместили.

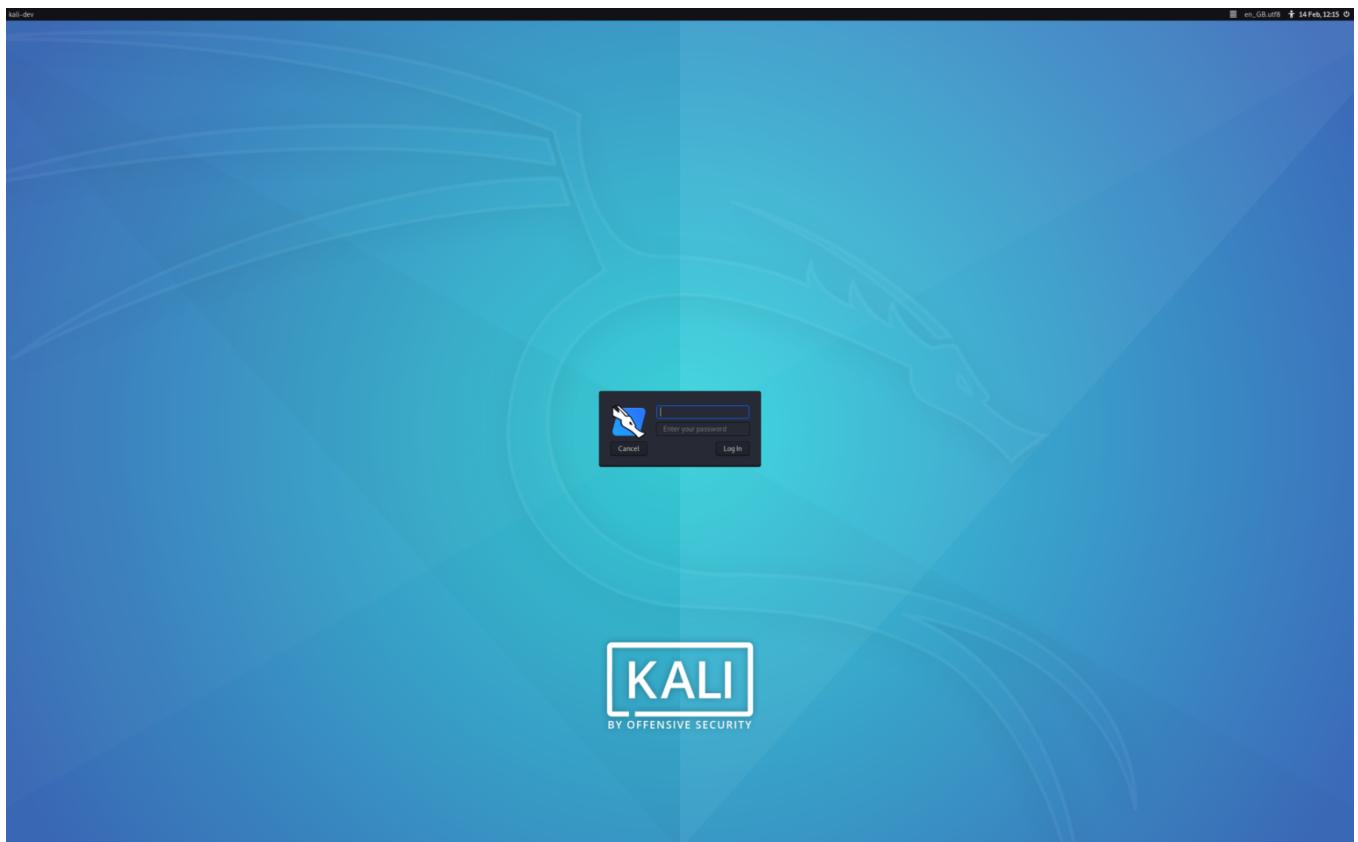
Чтобы решить эту проблему, вы можете изменить размер курсора с помощью следующей команды:

```
1 echo export XCURSOR_SIZE=48 >> ~/.xsessionrc
```

Примечание: возможно, вам придётся попробовать увеличить значение с 48.

## Экран входа в систему — LightDM

У вас возникла проблема с экраном входа в систему (**lightdm**), когда поле входа меньше «обычного»?



Возможное решение — установить для xft-dpi значение 180 (или выше):

```
1
2     grep xft-dpi /etc/lightdm/lightdm-gtk-greeter.conf
3     xft-dpi = 96
4
5     sudo vim /etc/lightdm/lightdm-gtk-greeter.conf
6
7     cat /etc/lightdm/lightdm-gtk-greeter.conf
8
9     [greeter]
10    ...
11    xft-dpi = 180
12    ...
13    ...
14
15
```

Примечание: возможно, вам придётся попробовать увеличить значение со 180.

## Режим Forensics (судебной экспертизы, IT криминалистики) в Kali Linux

Kali Linux «Live» предоставляет «криминалистический режим», функцию, впервые представленную в BackTrack Linux. Опция загрузки **Forensic mode live** («Криминалистический live режим») оказалась очень популярной по нескольким причинам:

- Kali Linux широко и легко доступен, многие потенциальные пользователи уже имеют Kali ISO или загрузочные USB-накопители.
- Когда возникает необходимость в судебной экспертизе, Kali Linux «Live» позволяет быстро и легко задействовать Kali Linux.
- Kali Linux поставляется с предустановленным самым популярным программным обеспечением с открытым исходным кодом для криминалистической экспертизы — удобным набором инструментов, когда вам нужно выполнить криминалистическую работу.



При загрузке в криминалистическом режиме загрузки происходит несколько очень важных изменений в нормальной работе системы:

1. Во-первых, внутренний жёсткий диск никогда не трогается. Если есть раздел подкачки, он не будет использоваться, и никакой внутренний диск не будет автоматически смонтирован. Мы проверили это, сначала взял стандартную систему и вынув жёсткий диск. Хеш-память диска была снята с помощью коммерческого пакета судебно-криминалистической экспертизы. Затем мы снова подключили диск к компьютеру и загрузили Kali Linux «Live» в криминалистическом режиме. После использования Kali в течение некоторого времени мы затем выключили систему, вынули жёсткий диск и снова сняли хеш. Эти хеши совпали, что указывает на то, что на диске ничего не менялось.
2. Другое, не менее важное изменение — отключение автоматического монтирования съёмных носителей. USB-

накопители, компакт-диски и т. п. не будут автоматически подключаться при установке. Идея этого проста: в криминалистическом режиме ничего не должно происходить ни с одним носителем без прямого действия пользователя. Всё, что вы делаете как пользователь, является вашей ответственностью.

Если вы планируете использовать Kali для реальной судебной экспертизы любого типа, мы не рекомендуем вам просто верить нам на слово. Все инструменты судебной экспертизы всегда следует проверять, чтобы вы знали, как они будут себя вести в любых обстоятельствах, в которых вы собираетесь их использовать. Наконец, хотя Kali продолжает фокусироваться на предоставлении лучшей коллекции доступных инструментов тестирования на проникновение с открытым исходным кодом, всегда возможно, что мы пропустили ваш любимый инструмент судебной экспертизы с открытым исходным кодом. Если да, дайте нам знать! Мы всегда ищем высококачественные инструменты с открытым исходным кодом, которые мы можем добавить в Kali, чтобы сделать этот дистрибутив ещё лучше.

## **Как установить драйверы для видеокарты NVIDIA**

Не пытайтесь сделать это на виртуальной машине. Теоретически это возможно, однако, скорее всего, это не сработает, и мы не рекомендуем пользователям пытаться это сделать.

В этом документе объясняется, как установить драйверы NVIDIA GPU и добавить поддержку CUDA, что обеспечивает интеграцию с популярными инструментами тестирования на проникновение.

Во-первых, вам нужно убедиться, что ваша карта поддерживает CUDA.

Рекомендуются графические процессоры с вычислительной способностью CUDA > 5.0, но графические процессоры с меньшим

количеством ресурсов все равно будут работать.

После этого убедитесь, что в ваших сетевых репозиториях включены **contrib** и **non-free** компоненты и что ваша система полностью обновлена:

```
1
2 sudo apt update
3 sudo apt -y full-upgrade -y
4 [ -f /var/run/reboot-required ] && sudo reboot -f
5
```

Давайте определим, какой именно графический процессор установлен, и проверим модули ядра, которые он использует:

```
1 lspci | grep -i -E '(vga|3d)'
```

Пример вывода:

```
1 00:02.0 VGA compatible controller: Intel Corporation UHD Graphics 630 (Mobile)
2 01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile] (rev a1)
```



The screenshot shows a terminal window titled 'mial@HackWare-Kali: ~'. The window contains the following text:

```
mial@HackWare-Kali: ~
Файл Действия Правка Вид Справка
(mail@HackWare-Kali)-[~]
$ lspci | grep -i -E '(vga|3d)'
00:02.0 VGA compatible controller: Intel Corporation UHD Graphics 630 (Mobile)
01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile]
(mail@HackWare-Kali)-[~]
$
```

С помощью опции **-v** можно увидеть больше подробностей, в том числе используемый драйвер ядра и модуль ядра. Чтобы ограничить вывод только интересующей нас видеокартой, используем опцию **-s [[[ДОМЕН]::]ШИНА]::[УСТРОЙСТВО].[ФУНКЦИЯ]]**. Эта опция означает показывать только устройства в указанном домене (если на

на вашем компьютере несколько хост-мостов, они могут использовать общее пространство номеров шины или каждый из них может адресовать собственный домен PCI; домены пронумерованы от 0 до ffff),шине (от 0 до ff), устройстве (от 0 до 1f) и функции (от 0 до 7). Каждый компонент адреса устройства может быть опущен или установлен на «\*», что означает «любое значение». Все числа шестнадцатеричные. Например, «**0:**» означает все устройства нашине 0, «**0**» означает все функции устройства 0 на любойшине, «**0.3**» выбирает третью функцию устройства 0 на всех шинах, а «**.4**» показывает только четвертую функцию каждого устройства. Нужно нам значением ("01:00.0") мы возьмём из предыдущего вывода команды **lspci**.

В следующей команде замените "01:00.0" на ваше значение:

Пример вывода:

```
1 01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050
2 Ti Mobile] (rev a1)
3
4     Subsystem: ASUSTeK Computer Inc. GP107M [GeForce GTX 1050 Ti
5 Mobile]
6
7     Flags: bus master, fast devsel, latency 0, IRQ 141, IOMMU
8 group 1
9
10    Memory at a3000000 (32-bit, non-prefetchable) [size=16M]
11
12    Memory at 90000000 (64-bit, prefetchable) [size=256M]
13
14    Memory at a0000000 (64-bit, prefetchable) [size=32M]
15
16    I/O ports at 5000 [size=128]
17
18    Expansion ROM at a4000000 [disabled] [size=512K]
19
20    Capabilities: <access denied>
21
22    Kernel driver in use: nouveau
23
24    Kernel modules: nouveau
```



```
mial@HackWare-Kali: ~
(mail@HackWare-Kali)-[~]
$ lspci -s 01:00.0 -v
01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile] (rev a1)
    Subsystem: ASUSTeK Computer Inc. GP107M [GeForce GTX 1050 Ti Mobile]
    Flags: bus master, fast devsel, latency 0, IRQ 141, IOMMU group 1
    Memory at a3000000 (32-bit, non-prefetchable) [size=16M]
    Memory at 90000000 (64-bit, prefetchable) [size=256M]
    Memory at a0000000 (64-bit, prefetchable) [size=32M]
    I/O ports at 5000 [size=128]
    Expansion ROM at a4000000 [disabled] [size=512K]
    Capabilities: <access denied>
    Kernel driver in use: nouveau
    Kernel modules: nouveau

(mail@HackWare-Kali)-[~]
$
```

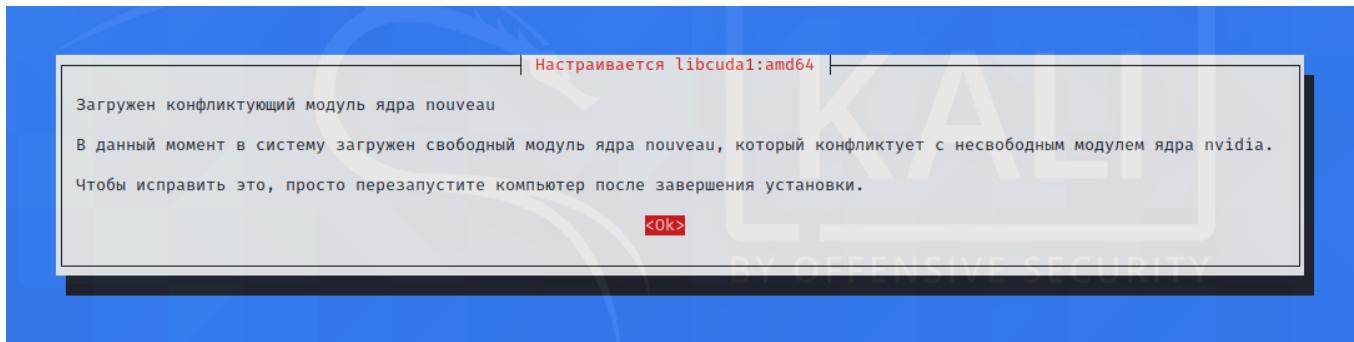
Обратите внимание, как **Kernel driver in use** и **Kernel modules** используют **nouveau**. Это драйвер с открытым исходным кодом для nVidia. В этом руководстве рассматривается установка драйвера с закрытым исходным кодом от NVIDIA.

Примечание: существует пакет под названием **nvidia-detect**, который не может обнаружить драйвер из-за того, что Kali является Rolling дистрибутивом, а **nvidia-detect** требует стабильного выпуска.

После перезагрузки системы после обновления ОС мы приступим к установке драйверов и инструментария CUDA (позволяющего инструментам для офлайн брут-форса использовать преимущества графического процессора).

Установка:

1	sudo apt install -y ocl-icd-libopencl1 nvidia-driver nvidia-cuda-toolkit
---	--



Во время установки драйверов в системе были созданы новые модули ядра, поэтому требуется перезагрузка:

После запуска Кали некоторые вещи могут выглядеть иначе, чем ожидалось.

- Если некоторые вещи меньше, это может быть из-за HiDPI.
- Однако, если некоторые объекты больше, это может быть связано с неправильным DPI.

Теперь, когда наша система должна быть готова к работе, нам нужно убедиться, что драйверы загружены правильно. Мы можем быстро проверить это, запустив инструмент [nvidia-smi](#).

Повторим команды, которыми мы смотрели свойства видеокарты:

```
1 lspci | grep -i -E '(vga|3d)'
```

Пример вывода:

1	00:02.0 VGA compatible controller: Intel Corporation UHD Graphics 630 (Mobile)
2	01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile] (rev a1)

```
mial@HackWare-Kali:~  
Файл Действия Правка Вид Справка  
└─(mial@HackWare-Kali)─[~]  
$ nvidia-smi  
Wed Jan 13 11:22:30 2021  
+-----+-----+-----+  
| NVIDIA-SMI 455.45.01      Driver Version: 455.45.01      CUDA Version: 11.1 |  
+-----+-----+-----+  
| GPU  Name      Persistence-M  Bus-Id      Disp.A  Volatile Uncorr. ECC |  
| Fan  Temp     Perf  Pwr:Usage/Cap | Memory-Usage | GPU-Util Compute M. |  
|          |          |          |          |          |          |          | MIG M. |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| 0  GeForce GTX 105 ... Off  00000000:01:00.0 Off   4MiB /  4042MiB | 0%       N/A | Default | N/A |  
| N/A   49C     P8    N/A / N/A |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
  
+-----+-----+-----+-----+-----+-----+  
| Processes:                               GPU Memory |  
| GPU  GI  CI      PID  Type  Process name        Usage |  
| ID   ID             |  
+-----+-----+-----+-----+-----+-----+-----+  
| 0    N/A N/A      827   G    /usr/lib/xorg/Xorg    4MiB |  
+-----+-----+-----+-----+-----+-----+-----+  
  
└─(mial@HackWare-Kali)─[~]  
$ lspci | grep -i -E '(vga|3d)'  
00:02.0 VGA compatible controller: Intel Corporation UHD Graphics 630 (Mobile)  
01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile] (rev a1)  
  
└─(mial@HackWare-Kali)─[~]  
$ lspci -s 01:00.0 -v  
01:00.0 3D controller: NVIDIA Corporation GP107M [GeForce GTX 1050 Ti Mobile] (rev a1)  
  Subsystem: ASUSTeK Computer Inc. GP107M [GeForce GTX 1050 Ti Mobile]  
  Flags: bus master, fast devsel, latency 0, IRQ 157, IOMMU group 1  
  Memory at a3000000 (32-bit, non-prefetchable) [size=16M]  
  Memory at 90000000 (64-bit, prefetchable) [size=256M]  
  Memory at a0000000 (64-bit, prefetchable) [size=32M]  
  I/O ports at 5000 [size=128]  
  Expansion ROM at a4000000 [virtual] [disabled] [size=512K]  
  Capabilities: <access denied>  
  Kernel driver in use: nvidia  
  Kernel modules: nvidia  
  
└─(mial@HackWare-Kali)─[~]  
$
```

Вы можете видеть, что наше оборудование было обнаружено, мы сейчас используем **nvidia**, а не драйвер  **nouveau**.

Теперь, когда на выходе правильно отображаются наш драйвер и графический процессор, мы можем погрузиться в бенчмаркинг (используя инструментарий CUDA). Прежде чем мы зайдём слишком далеко, давайте еще раз проверим, работают ли **hashcat** и CUDA вместе.

```
1 sudo apt install -y hashcat
```

Эта команда показывает, какие устройства видит [Hashcat](#):

Пример вывода:

```
mial@HackWare-Kali:~
```

Файл Действия Правка Вид Справка

CUDA Info:

=====

CUDA.Version.: 11.1

Backend Device ID #1 (Alias: #3)

Name.....: GeForce GTX 1050 Ti

Processor(s) ... : 6

Clock.....: 1620

Memory.Total ... : 4042 MB

Memory.Free....: 3992 MB

OpenCL Info:

=====

OpenCL Platform ID #1

Vendor..: Intel(R) Corporation

Name....: Intel(R) OpenCL HD Graphics

Version.: OpenCL 3.0

Backend Device ID #2

Type.....: GPU

Vendor.ID....: 8

Vendor.....: Intel(R) Corporation

Name.....: Intel(R) Graphics Gen9 [0x3e9b]

Version.....: OpenCL 3.0 NEO

Processor(s) ... : 24

Clock.....: 1100

Memory.Total ... : 25578 MB (limited to 4095 MB allocatable in one block)

Memory.Free....: 25514 MB

OpenCL.Version.: OpenCL C 3.0

Driver.Version.: 1.0.0

OpenCL Platform ID #2

Vendor..: NVIDIA Corporation

Name....: NVIDIA CUDA

Version.: OpenCL 1.2 CUDA 11.1.114

Backend Device ID #3 (Alias: #1)

Type.....: GPU

Vendor.ID....: 32

Vendor.....: NVIDIA Corporation

Name.....: GeForce GTX 1050 Ti

Version.....: OpenCL 1.2 CUDA

Processor(s) ... : 6

Clock.....: 1620

Memory.Total ... : 4042 MB (limited to 1010 MB allocatable in one block)

Memory.Free....: 3968 MB

OpenCL.Version.: OpenCL C 1.2

Driver.Version.: 455.45.01

OpenCL Platform ID #3

Vendor..: The pocl project

Name....: Portable Computing Language

Version.: OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL\_DEBUG

Backend Device ID #4

Type.....: CPU

Vendor.ID....: 128

Vendor.....: GenuineIntel

Похоже, всё работает, давайте продолжим и запустим встроенный тест производительности **hashcat**.

```
mial@HackWare-Kali:~
```

```
Файл Действия Правка Вид Справка
```

```
Hashmode: 0 - MD5
Speed.#1.....: 7246.1 MH/s (55.18ms) @ Accel:64 Loops:1024 Thr:1024 Vec:8
Speed.#2.....: 354.3 MH/s (66.96ms) @ Accel:256 Loops:512 Thr:8 Vec:4
Speed.#4.....: 592.6 MH/s (9.90ms) @ Accel:1024 Loops:512 Thr:1 Vec:8
Speed.#*.....: 8193.0 MH/s

Hashmode: 100 - SHA1
Speed.#1.....: 2397.5 MH/s (83.56ms) @ Accel:64 Loops:512 Thr:1024 Vec:1
Speed.#2.....: 141.7 MH/s (87.74ms) @ Accel:256 Loops:256 Thr:8 Vec:4
Speed.#4.....: 285.6 MH/s (42.52ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Speed.#*.....: 2824.8 MH/s

Hashmode: 1400 - SHA2-256
Speed.#1.....: 845.6 MH/s (59.13ms) @ Accel:16 Loops:512 Thr:1024 Vec:1
Speed.#2.....: 59253.5 kH/s (100.21ms) @ Accel:512 Loops:64 Thr:8 Vec:4
Speed.#4.....: 117.6 MH/s (51.69ms) @ Accel:1024 Loops:512 Thr:1 Vec:8
Speed.#*.....: 1022.5 MH/s

Hashmode: 1700 - SHA2-512
Speed.#1.....: 266.9 MH/s (93.98ms) @ Accel:8 Loops:512 Thr:1024 Vec:1
Speed.#2.....: 11560.0 kH/s (67.35ms) @ Accel:4 Loops:1024 Thr:8 Vec:1
Speed.#4.....: 39219.8 kH/s (79.84ms) @ Accel:1024 Loops:256 Thr:1 Vec:4
Speed.#*.....: 317.7 MH/s

Hashmode: 22000 - WPA-PBKDF2-PMKID+EAPOL (Iterations: 4095)
Speed.#1.....: 117.4 kH/s (104.47ms) @ Accel:16 Loops:512 Thr:1024 Vec:1
Speed.#2.....: 6714 H/s (55.27ms) @ Accel:32 Loops:256 Thr:8 Vec:1
Speed.#4.....: 9471 H/s (61.73ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Speed.#*.....: 133.5 kH/s

Hashmode: 1000 - NTLM
```

## Исправление проблем

Если установка идёт не так, как планировалось, мы установим [clinfo](#) для получения подробной информации по устранению неполадок.

```
1 sudo apt install -y clinfo
```

Запустим:

Загрузчики OpenCL: может потребоваться проверить наличие дополнительных пакетов, которые могут противоречить нашей настройке. Давайте сначала проверим, какой загрузчик OpenCL мы установили. Загрузчик NVIDIA OpenCL и стандартный загрузчик OpenCL будут работать в нашей системе.

```
(mial@HackWare-Kali)-[~]
$ dpkg -l | grep -i icd
ii intel-opencl-icd          20.44.18297-1
ii nvidia-egl-icd:amd64      455.45.01-1
ii nvidia-egl-icd:i386        455.45.01-1
ii nvidia-opencl-icd:amd64   455.45.01-1
ii nvidia-vulkan-icd:amd64   455.45.01-1
ii nvidia-vulkan-icd:i386    455.45.01-1
ii ocl-icd-libopencl1:amd64  2.2.13-1
ii ocl-icd-opencl-dev:amd64  2.2.13-1
ii pocl-opencl-icd:amd64     1.5-6
                            amd64      Intel graphics compute runtime for OpenCL
                            amd64      NVIDIA EGL installable client driver (ICD)
                            i386      NVIDIA EGL installable client driver (ICD)
                            amd64      NVIDIA OpenCL installable client driver (ICD)
                            amd64      NVIDIA Vulkan installable client driver (ICD)
                            i386      Generic OpenCL ICD Loader
                            amd64      OpenCL development files
                            amd64      pocl ICD

(mail@HackWare-Kali)-[~]
$
```

Если установлен **mesa-opencl-icd**, его следует удалить:

- 1 `dpkg -l | grep -i mesa-opencl-icd`
- 2 `sudo apt remove mesa-opencl-icd`

Поскольку мы определили, что у нас установлен совместимый загрузчик ICD, мы можем легко определить, какой загрузчик в настоящее время используется.

- 1 `clinfo | grep -i "icd loader"`

Как и ожидалось, наша установка использует загрузчик с открытым исходным кодом, который был установлен ранее. Теперь давайте получим некоторую подробную информацию о системе.

Запрос информации о графическом процессоре: мы снова будем использовать **nvidia-smi**, но с гораздо более подробным выводом.



```
mial@HackWare-Kali:~  
Файл Действия Правка Вид Справка  
└─(mial@HackWare-Kali)-[~]  
$ nvidia-smi -i 0 -q  
=====  
NVSMI LOG=  
  
Timestamp : Wed Jan 13 11:34:46 2021  
Driver Version : 455.45.01  
CUDA Version : 11.1  
  
Attached GPUs : 1  
GPU 00000000:01:00.0 :  
    Product Name : GeForce GTX 1050 Ti  
    Product Brand : GeForce  
    Display Mode : Disabled  
    Display Active : Disabled  
    Persistence Mode : Disabled  
    MIG Mode :  
        Current : N/A  
        Pending : N/A  
    Accounting Mode : Disabled  
    Accounting Mode Buffer Size : 4000  
    Driver Model :  
        Current : N/A  
        Pending : N/A  
    Serial Number : N/A  
    GPU UUID : GPU-e7cc6b38-164e-babb-d5e7-14b23d2e5e05  
    Minor Number : 0  
    VBIOS Version : 86.07.50.00.54  
    MultiGPU Board : No  
    Board ID : 0x100  
    GPU Part Number : N/A  
    Inforom Version :  
        Image Version : N/A  
        OEM Object : N/A  
        ECC Object : N/A  
        Power Management Object : N/A  
    GPU Operation Mode :  
        Current : N/A  
        Pending : N/A  
    GPU Virtualization Mode : None  
    Virtualization Mode :  
    Host VGPU Mode : N/A
```

Похоже, что наш графический процессор распознаётся правильно, поэтому давайте используем **glxinfo**, чтобы определить, включён ли 3D-рендеринг.

- 1 sudo apt install -y mesa-utils
- 2 glxinfo | grep -i "direct rendering"



```
mial@HackWare-Kali:~  
Файл Действия Правка Вид Справка  
└─(mial@HackWare-Kali)-[~]  
$ glxinfo | grep -i "direct rendering"  
direct rendering: Yes  
└─(mial@HackWare-Kali)-[~]  
$
```

Комбинация этих инструментов значительно облегчит процесс устранения неполадок. Если у вас все ещё возникают проблемы, мы рекомендуем поискать похожие настройки и любые нюансы, которые могут повлиять на вашу конкретную систему.

Смотрите также «**Включение OpenCL для Intel**» в разделе «[Установка видео драйверов в Linux](#)».

## Branch (ветки) Kali

### Что такое branch (ветка)?

Ветвь — это альтернативная версия некоторого программного обеспечения, в данном случае Kali OS. Kali Linux имеет несколько веток, которые позволяют пользователям решать, насколько актуальны их пакеты. Kali Linux во многом похож на Debian, в том числе подходом к использованию веток.

У вас может быть одновременно включено несколько веток. Однако переключение ветвей может вызвать проблемы, так как пакеты могут быть разных версий, а в некоторых случаях могут быть недоступны или нестабильны.

Смотрите страницу Сетевых репозиториев, чтобы узнать, как переключать ветки.

Начнём с основных веток, которые используются чаще всего и являются наиболее стабильными. Их часто считают «безопасными».

- **kali-rolling** — это основная ветка по умолчанию, которую следует использовать большинству пользователей. Она постоянно обновляется, поскольку она извлекается из **kali-dev** после обеспечения стабильности сомнительных пакетов и объединения их с пакетами из **kali-rolling-only**. Время от времени сюда может проскакивать проблемный пакет из-за ошибок в **debian-testing**.
- **kali-last-snapshot** — это ветвь Kali, которую можно

использовать, если пользователи хотят более стандартного ощущения управления программным обеспечением. Для каждого нового выпуска замораживается код и объединяются **kali-rolling** в **kali-last-snapshot**, после чего пользователи будут получать все обновления между выпусками с поддержкой версий (например, 2019.3 → 2019.4). Это часто более стабильно, так как пакеты не обновляются (до следующего выпуска, поскольку это «точечный выпуск») и проходят тестирование в рамках выпуска. Это самый «безопасный» вариант.

Далее идут те, которые вам, вероятно, не понадобятся, за исключением очень особых случаев:

- **kali-experimental** — это промежуточная область для незавершённых пакетов.
- **kali-bleeding-edge** содержит пакеты, которые автоматически обновляются из вышестоящих репозиториев git. Эта ветвь потенциально может быть очень нестабильной.

## Разработка

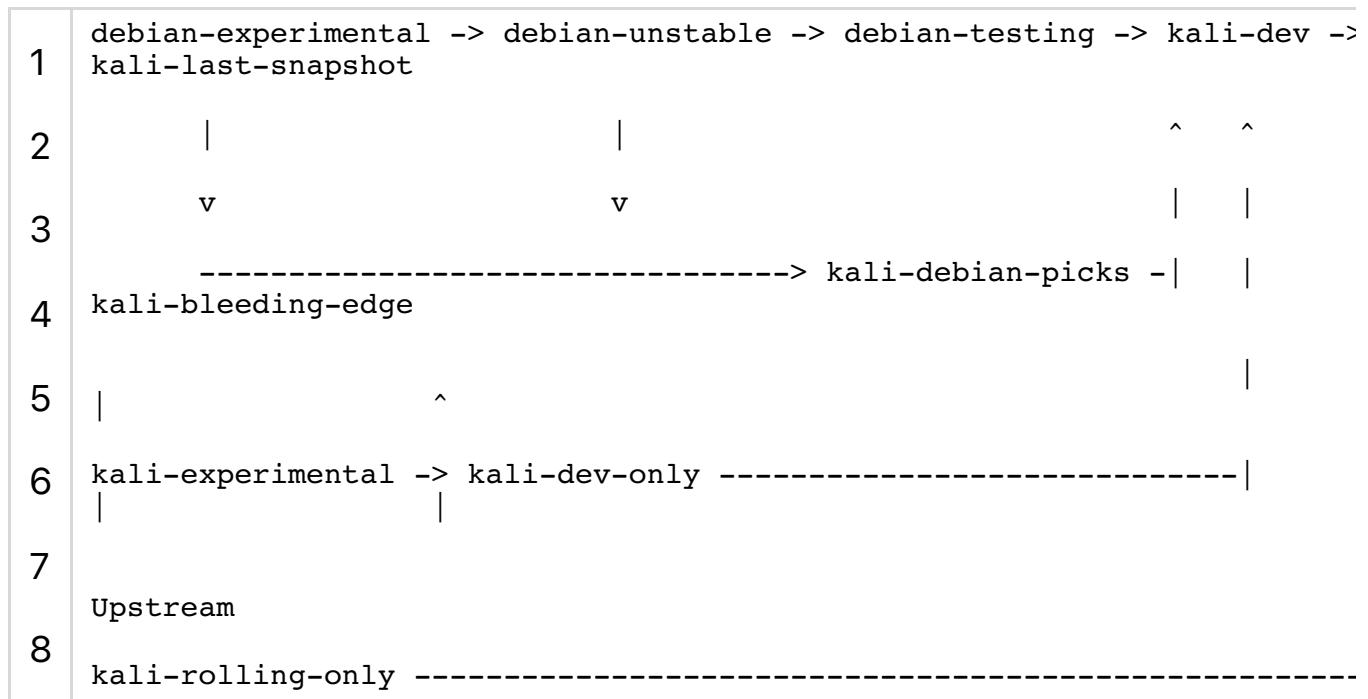
- **kali-dev** — это версия Kali в процессе разработки. Она создаётся путём объединения трёх других веток: **kali-dev-only**, **kali-debian-picks** и **debian-testing**. В основном она используется для слияния обновлений Debian с изменениями, поддерживаемыми Kali.
- **kali-dev-only** — пакеты в процессе разработки, специфичные для Kali. Эта ветка автоматически объединяется с **kali-dev**.
- **kali-rolling-only** — это репозиторий для пакетов, которым необходимо быстро достичь **kali-rolling**.

## Ветки, используемые для помощи другим веткам

- **kali-debian-picks** содержит пакеты, выбранные из **debian-experimental** и **debian-unstable**. Она автоматически сливаются с **kali-dev**.

- **debian-testing** — зеркало тестового дистрибутива Debian. Она используется для создания **kali-dev**.
- **debian-experimental** и **debian-unstable** — это частичные зеркала для определённых пакетов, которые мы хотим выбрать.

Ниже представлена диаграмма, показывающая взаимосвязь между ветвями.



## Связь с Debian

В Debian есть три основных варианта:

- **Stable**
- **Testing**
- **Unstable**

**Stable** — это «безопасная» ветвь Debian. Примерно каждые два месяца она обновляется «Точечным выпуском», который часто представляет собой просто обновления безопасности. Версии пакетов обычно не обновляются в это время из-за потенциальной несовместимости и, следовательно, нестабильности. Это Debian-эквивалент **kali-last-snapshot**.

**Testing** — это самое близкое к «rolling» дистрибутиву Debian, где

«rolling» означает, что как только доступно обновление пакета, оно выгружается. Kali использует эту ветку в качестве стартера для **kali-rolling** с января 2016 года.

**Unstable** — сразу после разработки пакета Debian. Пакеты созданы, но не полностью протестированы. Kali не имеет эквивалента, так как это rolling дистрибутив.

## Настройка Yubikeys для аутентификации SSH

В этом документе объясняется, как настроить Yubikey для аутентификации SSH.

Установите Yubikey Personalization Tool и Smart Card Daemon

```
1 sudo apt install -y yubikey-personalization scdaemon
```

Во-первых, вам необходимо убедиться, что ваша система полностью обновлена.

```
1 pcsc_scan
2 Scanning present readers...
3 Reader 0: Yubico Yubikey 4 OTP+U2F+CCID 00 00
4     Card state: Card inserted,
5 Possibly identified card (using /usr/share/pcsc-smartcard_list.txt):
6     Yubico Yubikey 4 OTP+CCID
```

Чтобы наш Yubikey определялся как смарт-карта, нам нужно установить наш Yubikey в режим CCID.

```
1
2 sudo ykpersonalize -m 86
3 The USB mode will be set to: 0x86
4 Commit? (y/n) [n]: y
```

После этой модификации GPG теперь сможет распознавать наш Yubikey как смарт-карту.

```
1 gpg --card-status
2 Reader .....: Yubico Yubikey 4 OTP U2F CCID 00 00
3 Version .....: 2.1
4 Manufacturer ....: Yubico
5 Key attributes ...: rsa2048 rsa2048 rsa2048
6 Max. PIN lengths .: 127 127 127
7 PIN retry counter : 3 0 3
```

Теперь нам нужно будет изменить настроенный PIN-код по умолчанию.

Примечание: PIN-код по умолчанию — 123456, а PIN-код администратора по умолчанию — 12345678.

```
1
2
3
4 gpg --change-pin
5 gpg: OpenPGP card no. F8482212202010006041587850000 detected
6 1 - change PIN
7 2 - unblock PIN
8 3 - change Admin PIN
9 4 - set the Reset Code
10 Q - quit
11 Your selection? 1
12 PIN changed.
```

```
12 1 - change PIN  
13 Your selection? 3  
14 PIN changed.  
15 Your selection? q  
16  
17  
18
```

## Программы, которые ведут себя иначе без прав root

Есть много пакетов, для использования которых требуются повышенные права. Есть также пакеты, которые могут работать без привилегированного доступа, но теряют часть своей функциональности. Эта страница будет постоянно обновляться, чтобы включать все инструменты, относящиеся к последней группе.

### Nmap

[Nmap](#) — один из наиболее распространённых инструментов, у которого есть нюансы при запуске без root и с правами root. В Nmap есть много разных методов сканирования, которые выполняют разные функции и используют разные методы для получения результатов. Одним из примеров этого является сканирование TCP SYN, которое использует сырые сокеты, доступные только пользователю root. Это сканирование выполняется по умолчанию, если вы являетесь привилегированным пользователем, в противном случае используется сканирование TCP-connect.

Разница между этими двумя сканированиями хорошо объяснена в разделе «[Виды сканирований Nmap](#)». Если коротко, SYN-сканирование является более незаметным и более быстрым, поскольку выполняет неполное соединение, а TCP-connect

завершает соединение полностью. У каждого есть свои преимущества или недостатки, поэтому хорошо понимать, что происходит с каждым из них.

## Настройка RDP с Xfce

Kali Linux поддерживается множеством различных устройств и систем. В некоторых из этих систем вы можете получить только базовую установку и иногда можете не иметь прямого доступа к графическому интерфейсу пользователя, например с WSL. Один простой способ получить доступ к графическому интерфейсу для Kali — это установить Xfce и настроить RDP. Это можно сделать вручную или с помощью предоставленного здесь скрипта, как показано ниже.

```
1
2 #!/bin/sh
3 echo "[+] Installing Xfce, this will take a while"
4 apt-get update
5 apt-get dist-upgrade -y --force-yes
6 apt-get install --yes --force-yes kali-desktop-xfce xorg xrdp
7 echo "[+] Configuring XRDP to listen to port 3390 (but not starting
8 the service)..."
9 sed -i 's/port=3389/port=3390/g' /etc/xrdp/xrdp.ini
```

Чтобы использовать скрипт, делаем следующее:

```
1
2 wget https://gitlab.com/kalilinux/build-scripts/kali-wsl-chroot/-/
3 /raw/master/xfce4.sh
4 chmod +x xfce4.sh
5 sudo ./xfce4.sh
```

Установка этого параметра вручную предоставит больший контроль над выполнением конфигурации, но также займет немного больше времени. После настройки Xfce и RDP вам необходимо запустить службу и подключиться. Для запуска службы вам необходимо запустить следующее:

```
1 sudo systemctl enable xrdp --now
```

Затем вы можете подключиться к этой системе с помощью клиента RDP. Запомните какой порт используется. Если вы использовали скрипт, порт будет **3390**. В случае WSL IP-адрес для подключения из вашей системы Windows **127.0.0.1:3390**.

## Кали в браузере (Guacamole)

Вы можете взаимодействовать с Kali различными способами, например, сидя прямо у компьютера с запущенной Kali (чаще всего с графическим интерфейсом), или используя Kali удалённо через SSH (что даёт вам доступ к командной строке). В качестве альтернативы вы можете настроить VNC, который обеспечит удалённый графический доступ (пожалуйста, убедитесь, что вы делаете это безопасно, заставив VNC прослушивать loopback и перенаправляя порт через SSH). Другой подход — взаимодействовать с Kali в браузере, вместо того, чтобы устанавливать необходимые клиенты VNC.

Это руководство охватывает Apache Guacamole, но у нас также есть другое руководство по VNC. У каждого есть свои плюсы и минусы. Guacamole — более полное решение, оно поддерживает несколько протоколов и позволяет клиентам подключаться к нему с центральной страницы с аутентификацией пользователя.

[Apache Guacamole не входит в пакет Debian](#) и содержит [различные шаги для завершения](#) настройки (или вы можете использовать [образ docker](#)). Имеется автоматизированный скрипт для установки.

## Первый этап — скачать скрипт:

```
1  
2 sudo apt update  
3 sudo apt install -y git  
4 git clone https://github.com/MysticRyuujin/guac-install.git  
/tmp/guac-install  
5
```

ВАЖНО! Если вы находитесь в восточном часовом поясе, вам придётся изменить его. В Apache есть ошибка, из-за которой EDT не рассматривается как действительный часовой пояс.

Чтобы решить эту проблему, мы изменим наш часовой пояс на Центральное время.

```
1 sudo rm /etc/localtime && sudo ln -s /usr/share/zoneinfo/US/Central  
/etc/localtime
```

Мы собираемся выполнить «автономную» установку, в которой не будет отдельного хоста базы данных MySQL, а также не будет включён какой-либо MFA (поскольку мы собираемся скрыть это за туннелем SSH):

```
1  
2 cd /tmp/guac-install/  
3 sudo ./guac-install.sh --nomfa --installmysql --mysqlpwd  
S3cur3Pa$$w0rd --guacpwd P@s$W0rD  
4 ...SNIP...  
5 Cleanup install files...  
6 Installation Complete  
7 - Visit: http://localhost:8080/guacamole/  
8 - Default login (username/password): guacadmin/guacadmin  
9 ***Be sure to change the password***.
```

Можем оперативно проверить, все ли службы счастливы:

```
1
2
3     systemctl status tomcat9 guacd mysql
4
5         ● tomcat9.service - Apache Tomcat 9 Web Application Server
6             Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled;
7                 vendor preset: disabled)
8
9                 Active: active (running) since Thu 2020-03-05 17:39:38 GMT; 1min
10                14s ago
11
12                   Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
13
14               Main PID: 33192 (java)
15
16               Tasks: 47 (limit: 19107)
17
18               Memory: 454.8M
19
20               CGroup: /system.slice/tomcat9.service
21
22
23                     └─33192 /usr/lib/jvm/default-java/bin/java -
24                         Djava.util.logging.config.file=/var/lib/tomcat9/conf/logging.properties
25                         -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
26                         Djava.awt.headless=true
27
28
29         ● guacd.service - LSB: Guacamole proxy daemon
30
31             Loaded: loaded (/etc/init.d/guacd; generated)
32
33             Active: active (running) since Thu 2020-03-05 14:04:34 GMT; 3h
34                 36min ago
35
36                   Docs: man:systemd-sysv-generator(8)
37
38                   Tasks: 1 (limit: 19107)
39
40                   Memory: 11.5M
41
42                   CGroup: /system.slice/guacd.service
43
44
45                     └─991 /usr/local/sbin/guacd -p /var/run/guacd.pid
46
47
48             Warning: Journal has been rotated since unit was started. Log output :
49                 incomplete or unavailable.
50
51
52         ● mysql.service - LSB: Start and stop the mysql database server daemon
53
54             Loaded: loaded (/etc/init.d/mysql; generated)
```

```
23      Active: active (running) since Thu 2020-03-05 17:39:46 GMT; 1min
24      6s ago
25
26      Docs: man:systemd-sysv-generator(8)
27
28      Tasks: 34 (limit: 19107)
29
30      Memory: 88.9M
31
32      CGroup: /system.slice/mysql.service
33
34          └─33670 /bin/sh /usr/bin/mysqld_safe
35
36          ├─33787 /usr/sbin/mysqld --basedir=/usr --
37          |   datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-
38          |   gnu/mariadb19/plugin --user=mysql --skip-log-error --pid-
39          |   file=/run/mysqld/mysqld.pid --soc>
40
41          └─33788 logger -t mysqld -p daemon error
42
43
44      sudo ss -antup | grep "mysqld\|guacd\|java"
45
46      tcp      LISTEN    0        80           127.0.0.1:3306
47      0.0.0.0:*      users:(( "mysqld", pid=33787, fd=21 ))
48
49      tcp      LISTEN    0        5            127.0.0.1:4822
50      0.0.0.0:*      users:(( "guacd", pid=991, fd=4 ))
51
52      tcp      LISTEN    0        100          *:8080
53      *:*      users:(( "java", pid=33192, fd=36 ))
54
55
56
```

Все службы работают правильно.

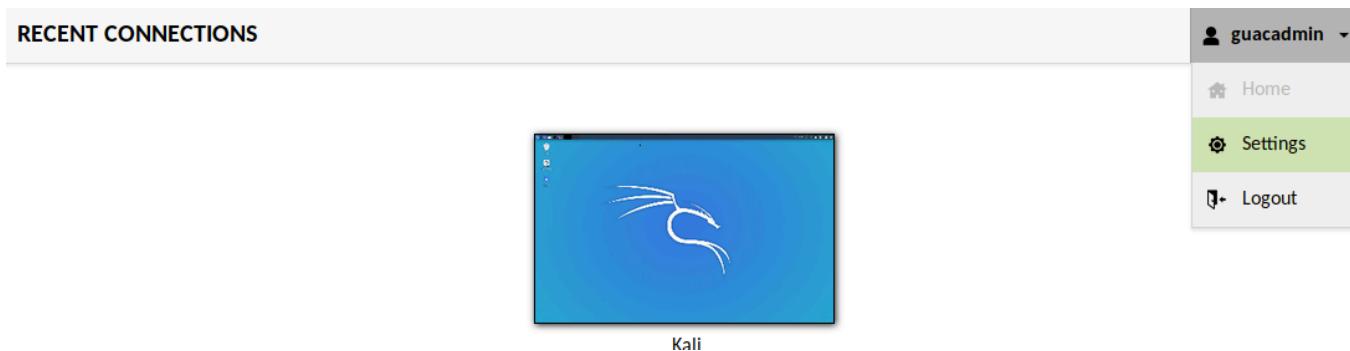
Далее следует включить службу VNC на Kali.

Мы собираемся использовать TigerVNC.

```
1
2      sudo apt install -y tigervnc-standalone-server
3
4      mkdir ~/.vnc/ && wget https://gitlab.com/kalilinux/nethunter/build-
5      scripts/kali-nethunter-project/-/raw/master/nethunter-
6      fs/profiles/xstartup -O ~/.vnc/xstartup
7
8      vncserver :1
```

Далее мы собираемся перейти в административную панель гуакамоле и создать новое соединение.

Сначала мы нажимаем «Настройки» в правом верхнем раскрывающемся меню.



Затем мы перейдём на вкладку «Подключения» и нажмём «Новое подключение». Мы заполним эти поля ниже:

Name:

Location:

Protocol:

#### CONCURRENCY LIMITS

Maximum number of connections:

Maximum number of connections per user:

#### LOAD BALANCING

Connection weight:

Use for failover only:

#### GUACAMOLE PROXY PARAMETERS (GUACD)

Hostname:

Port:

Encryption:

#### PARAMETERS

##### Network

Hostname:

Port:

##### Authentication

Password:

##### Display

Read-only:

Swap red/blue components:

Cursor:

Color depth:

Мы обязательно устанавливаем «Глубину цвета», мы делаем это, чтобы цвета проходили правильно. При неправильной настройке некоторые оттенки серого могут стать пурпурными или другими.

После всего этого вы можете перейти в «Домой» из верхнего правого раскрывающегося списка и щёлкнуть новое соединение.

## Kali в браузере (noVNC)

Вы можете взаимодействовать с Kali различными способами, например, сидя прямо у компьютера с запущенной Kali (чаще всего с графическим интерфейсом), или используя Kali удалённо через SSH

(что даёт вам доступ к командной строке). В качестве альтернативы вы можете настроить VNC, который обеспечит удалённый графический доступ (пожалуйста, убедитесь, что вы делаете это безопасно, заставив VNC прослушивать loopback и перенаправляя порт через SSH). Другой подход — взаимодействовать с Kali в браузере, вместо того, чтобы устанавливать необходимые клиенты VNC.

Это руководство охватывает noVNC, но у нас также есть другое руководство для Apache Guacamole. У каждого есть свои плюсы и минусы. NoVNC — это более лёгкий подход, поскольку он требует меньше служб (меньше накладных расходов), что позволяет быстро получить решение «одноразовое подключение».

Сначала мы обновляем, а затем устанавливаем необходимые пакеты (мы выбрали [x11vnc](#) в качестве нашего решения VNC. Вы можете переключить его на любой сервис VNC по вашему желанию. Однако поддержка может быть разной):

```
1 sudo apt update
2
3 sudo apt install -y novnc x11vnc
```

Затем мы запускаем сеанс VNC. Мы решили сделать это только на loopback, что сделало соединение более безопасным (мы пропускаем встроенную функцию HTTP x11vnc. Для этого требуется Java, и мы не хотим устанавливать её ни на одном из наших клиентов, поскольку noVNC даёт возможность работать с HTML5) :

```
1 x11vnc -display :0 -autoport -localhost -nopw -bg -xkb -ncache -
2 ncache_cr -quiet -forever
3 The VNC desktop is:      localhost:0
4 PORT=5900
```

**ПРИМЕЧАНИЕ.** Мы используем **display :0**, который является нашим текущим рабочим столом.

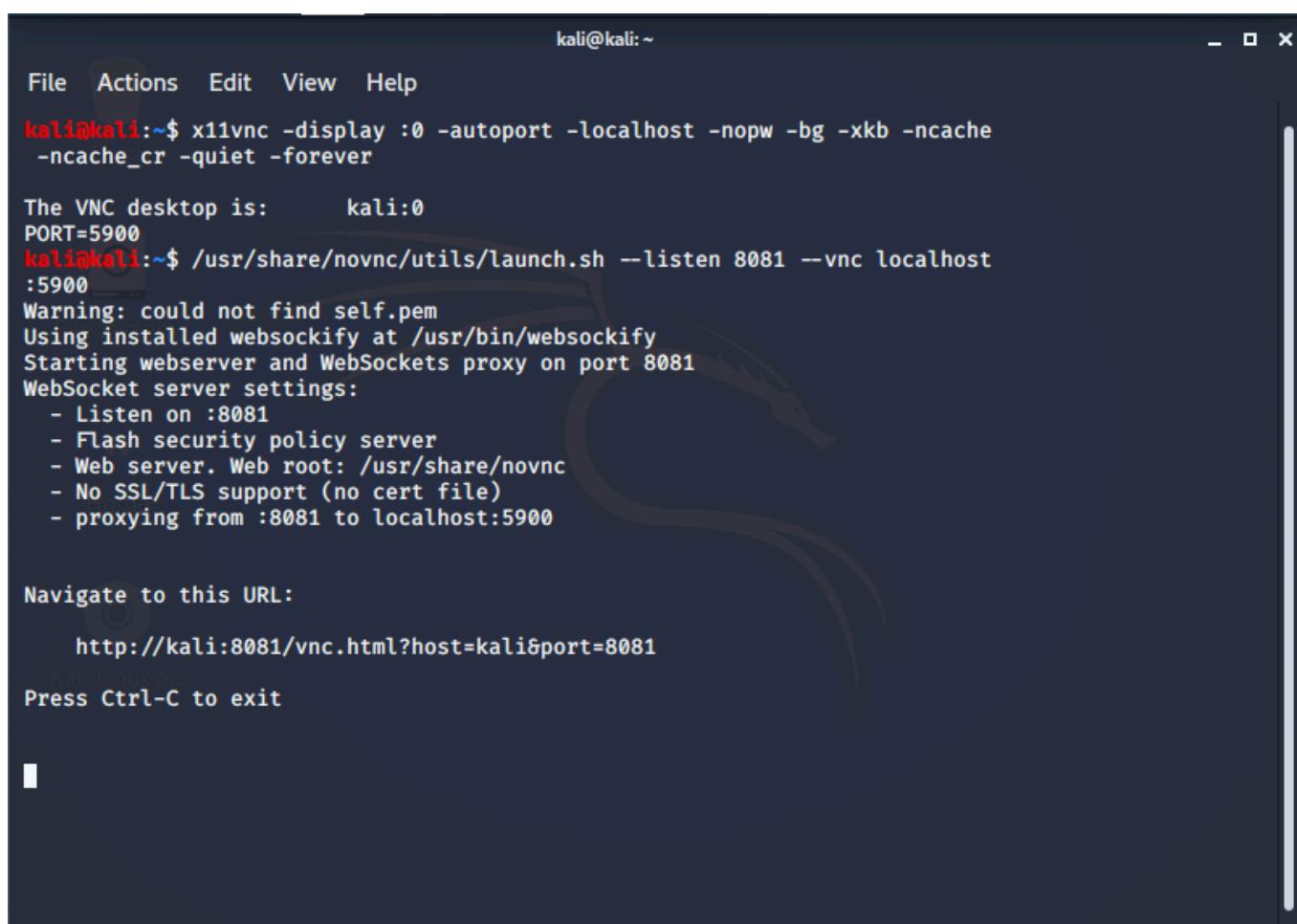
Мы можем проверить, какой порт используется для VNC:

```
1 ss -antp | grep vnc
2 LISTEN      0      32          127.0.0.1:5900
2 0.0.0.0:*      users:(("x11vnc",pid=8056,fd=8))
3 LISTEN      0      32          [::]:5900
3 [::]:*      users:(("x11vnc",pid=8056,fd=9))
```

Мы видим, что служба использует порт 5900.

После этого мы запускаем noVNC (она откроет **8081/TCP**):

```
1 /usr/share/novnc/utils/launch.sh --listen 8081 --vnc localhost:5900
```



The screenshot shows a terminal window titled "kali@kali:~". The user has run the command `/usr/share/novnc/utils/launch.sh --listen 8081 --vnc localhost:5900`. The output indicates that the VNC desktop is at port 5900, and the noVNC web server is starting on port 8081. It provides details about the WebSocket server settings, including listening on port 8081, using a Flash security policy server, and proxying from port 8081 to port 5900. A URL is provided for navigation: `http://kali:8081/vnc.html?host=kali&port=8081`.

А ещё лучше включите SSH:

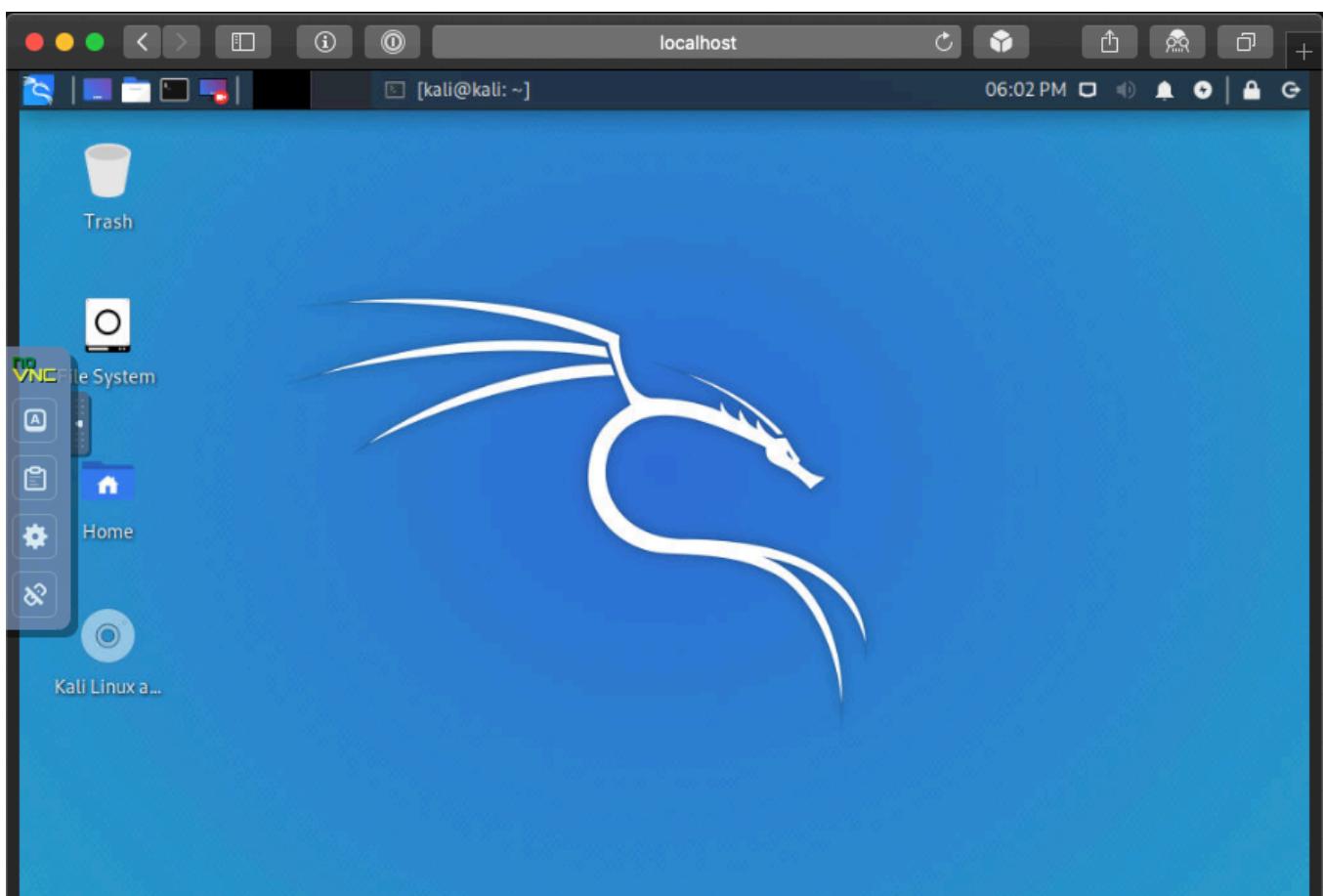
```
1 sudo systemctl enable ssh
```

```
2 sudo systemctl start ssh
```

```
3
```

Затем на удалённом компьютере введите SSH в вашу настройку Kali (вам может потребоваться сначала включить переадресацию портов)

```
1 ssh kali@192.168.13.37 -L 8081:localhost:8081
```



## Домены Kali

В Kali есть несколько поддоменов, о которых может быть полезно знать:

**<https://www.kali.org/>**: Официальный сайт Kali Linux! Пользователи могут найти ссылки на загрузки, блог, обучение, документацию и многое другое.

**<https://www.kali.org/docs/>**: здесь находится официальная документация по Kali Linux. Пользователи могут найти документацию от начальной установки до того, как создать Live USB с поддержкой

LUKS Nuke.

**<https://tools.kali.org/>**: на многие вопросы, связанные с пакетами, можно ответить, просмотрев этот сайт. Этот сайт и [pkg.kali.org](https://pkg.kali.org) хранят большую часть информации о версиях пакетов, о том, какие инструменты в каких метапакетах, справочные страницы инструментов и многое другое. Инструменты содержат информацию о случаях использования инструмента.

**<https://kali.training/>**: Новые или опытные пользователи Kali могут пожелать получить больше знаний о Kali, о которой рассказывается на этом сайте. Kali Training позволяет пользователям прочитать книгу *Kali Linux Revealed* и выполнять практические тесты, связанные с содержанием глав. Это всё для подготовки к экзамену KLCP (Kali Linux Certified Professional).

**<https://bugs.kali.org/>**: каждый раз, когда у пользователя возникает проблема, которая точно является ошибкой, он может сообщить об этой ошибке в нашу систему отслеживания ошибок.

**<https://forums.kali.org/>**: сайт, на который пользователи могут прийти, когда им понадобится помочь. Вопросы, касающиеся оборудования, программного обеспечения и общей информации, связанной с Kali, обсуждаются с другими членами сообщества.

**<https://autopkgtest.kali.org/>**: многие пакеты имеют связанный с ними тест, чтобы гарантировать их выполнение. На этом сайте показаны все эти тесты и показано, проходят ли эти пакеты тесты.

**<https://pkg.kali.org/>**: аналог [tools.kali.org](https://tools.kali.org/), очень полезный для пользователей, позволяющий просматривать историю пакета. Наряду с историей пользователи могут видеть связанные двоичные файлы, апстрим, пакет в репозитории Kali git и многое другое. Ещё одна полезная функция, о которой следует знать, — это возможность отслеживать версии пакетов, что можно сделать по электронной почте или через RSS-канал. Это хорошо объясняется в документации

Debian по программному обеспечению.

**<http://old.kali.org/>**: Если по какой-либо причине пользователю нужна старая копия Kali Linux, то этот сайт для них. Можно найти образы некоторых из первых выпусков Kali, а также более поздних выпусков.

**<https://http.kali.org/>**: URL-адрес перенаправителя для зеркал, доступных Kali. Он должен указывать на ближайшее к вам зеркало.

**<https://cdimage.kali.org/>**: сервер, на котором размещены ISO для загрузки.

**<https://status.kali.org/>**: если какой-либо сайт у вас не работает, вы можете проверить его статус здесь.

## **Сетевые репозитории Kali (/etc/apt/sources.list)**

Тема репозиториев всегда обширна и поднимается часто. Это предмет, с которым люди часто ошибаются и путаются. Пожалуйста, найдите время, чтобы прочитать информацию ниже и информацию по ссылкам в этом разделе, прежде чем что-либо предпринимать.

### **Официальный репозиторий Kali Linux**

При стандартной чистой установке Kali Linux с доступом к сети у вас должна быть следующая запись в **/etc/apt/sources.list**:

```
1  grep -v '#' /etc/apt/sources.list | sort -u
2
3  deb http://http.kali.org/kali kali-rolling main non-free contrib
```

Если результат не совсем соответствует приведённому выше, возможно, вы не сможете установить какие-либо новые дополнительные пакеты или получать обновления. Это может произойти по любому количеству причин, например:

- Вы выполнили установку в автономном режиме (например, при отсутствии сетевого подключения во время установки).
- Вы сменили ветку.
- Использование другого (жёстко запрограммированного) зеркала. Вы, вероятно, захотите прочитать следующий раздел «**Переключение ветвей/обычных репозиториев**», чтобы изменить это.

## Переключение ветвей/обычных репозиториев

Kali имеет различные ветви на выбор (пожалуйста, найдите время, чтобы прочитать, какая из них будет лучшим вариантом для вашей установки), и вы можете переключить или включить дополнительные репозитории.

Включение **kali-rolling** (ветка по умолчанию и часто обновляется):

```
1 echo "deb http://http.kali.org/kali kali-rolling main non-free contrib" | sudo tee /etc/apt/sources.list
```

Включение **kali-last-snapshot** (Точечный выпуск, более «стабильный» и «самый безопасный»):

```
1 echo "deb http://http.kali.org/kali kali-last-snapshot main non-free contrib" | sudo tee /etc/apt/sources.list
```

Включение **kali-experimental** (Пакеты, которые находятся в стадии тестирования — часто используются с rolling репозиторием)

```
1 echo "deb http://http.kali.org/kali kali-experimental main non-free contrib" | sudo tee -a /etc/apt/sources.list
```

Вам не нужно включать сразу их все — выберите одну из них, подходящую в большей степени.

## Формат файла sources.list

```
1 deb http://http.kali.org/kali kali-rolling main non-free contrib
```

- **Архив** будет **deb** (обычный двоичный) или **deb-src** (исходный код), в зависимости от того, нужен ли вам пакет или его исходный код.
- **Зеркало** должно быть <http://kali.org/kali>, так как это балансировщик нагрузки, который направит вас к лучшему зеркалу.
- **Ветка** — это то, какую версию Kali вы хотите использовать.
- **Компонент** — это пакеты, которые вы хотите использовать, в соответствии с [Руководством по свободному программному обеспечению Debian \(DFSG\)](#). Kali соответствует всему.

## Значения по умолчанию при автономной установки

Если в процессе установки Kali у вас нет доступа к сетевому подключению для доступа к репозиторию, вы выполните установку Kali в автономном режиме. Вы будете ограничены пакетами и версией, которые находятся на носителе, с которого вы установили Kali. Затем установщик настроит Kali для продолжения использования этого носителя для установки пакетов даже после завершения установки Kali. Это означает, что вы не получите никаких обновлений пакетов или каких-либо новых дополнительных инструментов, что может расстраивать. Вы можете увидеть, включён ли автономный носитель, если ваши значения соответствуют приведённым ниже (или если вы хотите включить эту опцию):

```
1 cat /etc/apt/sources.list
```

Пример вывода (обратите внимание на строки, содержащие слово **cdrom**):

Добавление диска в список источников Debian **apt**:

Пример вывода:

```
Using CD-ROM mount point /media/cdrom/
```

```
1 Identifying... [ea19ff4bedaa6c8f4662c0e8c58ed44c-2]
2 Scanning disc for index files...
3 Found 2 package indexes, 0 source indexes, 0 translation indexes and
0 signatures
4 This disc is called:
5 'Kali GNU/Linux 2020.1a _Kali-last-snapshot_ - Official amd64 DVD
Binary-1 with firmware 20200213-14:56'
6 Reading Package Indexes... Done
7 Writing new source list
8 Source list entries for this disc are:
9 deb cdrom:[Kali GNU/Linux 2020.1a _Kali-last-snapshot_ - Official
amd64 DVD Binary-1 with firmware 20200213-14:56]/ kali-rolling main
10 non-free
11 Repeat this process for the rest of the CDs in your set.
```

Если ваш вывод совпадает с указанным выше, смотрите чуть выше раздел **«Переключение ветвей/обычных репозиториев»**, если вы хотите получать обновления. Однако, если во время установки у вас есть сетевое соединение, которое имеет доступ к сетевым репозиториям, оно будет включено для вас. Вам не нужно ничего делать если вы устанавливали Kali Linux не онлайн.

Материал по теме: [Как добавить блочное устройство cdrom в список источников Debian apt](#)

## Репозитории не Kali

Если вы хотите установить дополнительные инструменты и программное обеспечение (например, [signal](#)) помимо того, что предлагает Kali, для этого вам может потребоваться включить дополнительный репозиторий. Пожалуйста, не изменяйте **/etc/apt/sources.list**, так как он используется для операционной системы Kali Linux. Любые дополнительные инструменты и программное обеспечение необходимо поместить в отдельный файл

в каталоге `/etc/apt/sources.list.d/` (например, `/etc/apt/sources.list.d/repo-name.list`, заменив **repo-name** на имя зеркала). Настоятельно рекомендуется, чтобы каждое зеркало было в отдельном файле. При добавлении репозитория Kali в ОС, отличную от Kali (например, при попытке добавить Kali в Ubuntu), это значительно увеличит вероятность того, что ваша система не будет работать. Это может произойти не сразу, но всё может сломаться без предупреждения. Мы не сможем предложить поддержку (и, судя по тому, что мы видели за эти годы, большинство других ОС тоже не помогут). Точно так же, добавление репозиториев других операционных систем в Kali (например, попытка поставить Ubuntu на Kali), сломает вашу установку. Это единственная наиболее распространённая причина, по которой системы Kali Linux ломаются. Если какие-либо руководства говорят вам по-другому, а не как это сказано здесь, это неофициальный совет и полностью не поддерживается Kali Linux. Чаще всего после подобных инструкций пользователи выполняют переустановку своей операционной системы.

## Зеркала

У нас есть [список официальных зеркал Kali Linux](#), а также [руководство по настройке собственного](#). Оно может храниться как локальный репозиторий, доступный только в локальной сети, или как удалённый частный, или, если у вас есть возможность, вы можете захотеть поделиться с сообществом и [сделать его общедоступным](#), позволяя пользоваться им всем пользователям в вашем географическом регионе.

## Репозитории исходного кода

Использование **deb** в репозиториях позволит загружать бинарные пакеты. Однако, если вам потребуется исходный код для пакета (чтобы вы могли скомпилировать пакет самостоятельно, если хотите, или заняться отладкой проблемы с пакетом), вы можете добавить **deb-src** в качестве дополнительной строки в репозитории.

```
1 echo "deb-src http://http.kali.org/kali kali-rolling main non-free  
contrib" | sudo tee -a /etc/apt/sources.list
```

В вышеприведённой команде мы использовали ветку **kali-rolling**, но вы можете выбрать любое значение, которое хотите.

## Kali Training

### Что такое Kali Training?

Kali Training — это официальный сайт книги о Kali — Kali Linux Revealed. Kali Training позволит вам изучить материал книги и сдать практические экзамены, чтобы проверить свои знания по главам из книги. Книга охватывает темы от установки Kali и базовых требований до перекомпиляции ядра.

Пользователям предлагается прочитать и сдать практические экзамены, чтобы получить полезные знания по многим аспектам Kali. Ежедневные задачи могут быть ускорены, всплывающие проблемы могут быть легко выявлены и потенциально исправлены, и после завершения книги может быть получено хорошее понимание того, что происходит под капотом ОС.

### Что мне делать дальше?

После прохождения всего тренинга Kali и практического теста можно получить следующий сертификат. Сертификат Kali Linux Certified Profession (KLCP) — это признание того, что вы знакомы с Kali Linux, многими основами Linux и некоторыми более продвинутыми функциями Linux.

## Переключение среды рабочего стола

Во время установки пользователь может выбрать любую среду рабочего стола, которую он предпочитает. Однако при использовании официальной виртуальной машины это невозможно. В этих и многих других случаях пользователь может захотеть

изменить среду своего рабочего стола.

Это делается очень просто — достаточно установить соответствующий метапакет. Их названия вы найдёте на странице [«Метапакеты Kali Linux»](#) в разделе **«Окружения рабочего стола/оконные менеджеры»**. Общий вид их имени: **kali-desktop-\***.

В качестве примера следующей командой устанавливается KDE:

- 1 sudo apt update
- 2 sudo apt install -y kali-desktop-kde

Для разных сред рабочего стола используются разные x-session-manager, они устанавливаются автоматически, но нужно выбрать тот, который будет использоваться по умолчанию. Это делается командой:

- 1 sudo update-alternatives --config x-session-manager

Для KDE выберите «sddm».

Если мы решим установить KDE, мы должны помнить о нескольких конфликтах, которые могут возникнуть. Мы можем установить KDE вместе с другими графическими окружениями рабочего стола, однако способ, которым в настоящее время настроены пакеты, может вызвать несколько конфликтов конфигурации. Например, если установлены и KDE, и Xfce, в Xfce возникают проблемы с курсором.

Чтобы обойти это, мы удалим Xfce и установим только KDE, и мы не советуем иметь вместе с ним другие окружения рабочего стола. Имейте в виду, что это применимо только для KDE; у вас могут быть установлены одновременно Xfce и GNOME и при этом не возникнет никаких конфликтов.

- 1 sudo apt purge --autoremove kali-desktop-xfce

Теперь мы перезагрузим систему и убедимся, что все наши

изменения были внесены правильно.

## Обновление Kali

### Когда стоит обновить Kali?

Если у вас установлена Kali по умолчанию, вам следует проверять наличие обновлений каждые несколько недель. Если вам нужна новая версия инструмента или вы узнали об обновлении безопасности, то это может ускорить график. Однако перед выполнением важных задач рекомендуется убедиться, что все инструменты работают, и не нужно обновляться пока эта важная задача не завершена. Поскольку Kali является rolling выпуском, время от времени возникают проблемы, которые могут привести к поломке необходимого инструмента.

Если вы используете ветку **last-snapshot**, вы не будете получать обновления, пока не будет выпущена следующая версия Kali для этого года. По этой причине рекомендуется следить за Kali Twitter или проверять веб-сайт Kali каждые несколько месяцев. Kali выпускается четыре раза в год и следует чёткому ежеквартальному графику.

### Как обновить Кали?

Чтобы обновить Kali, сначала убедитесь, что `/etc/apt/sources.list` правильно заполнен:

```
1 cat /etc/apt/sources.list
```

Вывод:

```
1 deb http://http.kali.org/kali kali-rolling main contrib non-free
2 deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

После этого мы можем запустить следующие команды, которые обновят нас до последних версий Kali:

1 sudo apt update

2 sudo apt full-upgrade -y