ALICIA NOORS
MARK B.

HACKING WITH PYTHON AND KALI-LINUX

DEVELOP YOUR OWN HACKINGTOOLS WITH PYTHON IN KALI-LINUX

```
          n/python3
          s, time
          cket as s

if len(sys.argv) != 3:
 print("USAGE:")
 print("./" + sys.argv[0] + " [IP] [STARTPORT-ENDPORT] \n")
 sys.exit()

ip = sys.argv[1]
ports = sys.argv[2].split("-")

 soc.settimeout(6)
 res = soc.connect_ex((ip, port))

 if res == 0:
  banner = ""
  if port == 80:
   soc.send(b'GET / HTTP/1.1 \r\n')
  try:
   banner = soc.recv(1024)
   banner = banner.decode("UTF-8", errors="replace").strip()
   if port == 80:
    tmp = banner.split("\n")
    for line in tmp:
     if line.strip().lower().startswith("server"):
      banner = line.strip()
  except:
      pass

   print("Port " + str(port) + " OPEN [" + banner + "]")

  soc.close()
```

ALICIA NOORS
MARK B.

HACKING WITH PYTHON AND KALI-LINUX

DEVELOP YOUR OWN HACKINGTOOLS WITH PYTHON IN KALI-LINUX

IMPRINT

Bibliographic information from the German National Library:
The German National Library lists this publication in the German National Bibliography; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de.

Production and publishing:
BoD – Books on Demand, Norderstedt

ISBN:
978-3752699913

PREFACE

When I got my first computer, a new and fascinating world opened up to me. Soon become "operating" the machine too boring for me and I was thirsty to find out exactly how this thing worked...

When I discovered QBasic on my computer and started to learn programming with the help of a few books, I was gripped by a fascination that has remained with me to this day. While my classmates used their computers to play games, I was tinkering with my programs for days and weeks.

I quickly realized - that is exactly what I want to do later. When I finally started to work in software development, I soon came across the topic of security and again a fascinating new world opened up to me - a world full of puzzles and riddles that had to be solved.

Over time, puzzling how a piece of software can be "outwitted" and looking for vulnerabilities in programs and websites became even more fun than development.

I hope that in this book I can bring you a little closer to my fascination for the topics of hacking and programming and maybe infect you with the same "virus" that grabbed me years ago and never let go...

So, I hope you enjoy our book!

Yours

Alicia Noorz

TABLE OF CONTENTS

WHY PYTHON

Python is a programming language that is not only easy to learn and more than fully documented, but also has an almost infinite number of modules that you can use in your own program and that provide functions for all imaginable tasks.

So it is possible to write a tool with just a few lines of code to automate a certain task. This is exactly why Python is so popular. Of course, there are many hacking tools for all kinds of tasks - but it is often faster to write a few lines in Python than to search the Internet for a suitable program.

Furthermore, blindly executing any tool found on underground or darknet forums without first inspecting the code is not necessarily the best idea. It is not uncommon for tools offered in forums and hacking sites to come with a nasty surprise. If you don't want to integrate your computer into the botnet of the tool-author, you should at least be able to understand the code of a script and check what exactly it does.

Apart from that, in my opinion, the quickest way to understand how an attack or a certain tool works is to recreate it yourself.

KALI-LINUX - INSTALLATION & SETUP

Kali is a so-called pentesting distribution - i.e. a system that already contains the most popular hacking tools and various tools for software development.

So I will use Kali-Linux as the base platform for the examples in this book. You are of course free to install the required tools on the operating system of your choice. At this point, I will only deal with the installation of Kali and the setup of various tools under Kali, as I assume that for people who are interested in the subject of this book, installing software under the operating system of their choice can not present any difficulty.

Kali can be downloaded free of charge from `https://www.kali.org/downloads/`. Those who want to use a virtual PC can download ready-made VMware or VirtualBox images.

Besides to Kali-Linux with Gnome3 the window-managers KDE, XFCE4, LXDE, Enlightenment and Mate are offered as an alternative. For those who do not know Linux - the window manager is, to put it simply, the graphical user interface of the system, and with Linux, you can choose which one to use. But don't confuse this with themes as you know from other operating systems! The individual window managers differ not only in appearance but also in resource consumption, the operating concept and the standard tools (settings management, file manager, etc.) that are included.

For my part, I prefer XFCE. The look is clean and simple, the window manager is resource-saving and optimized for fast work. Besides, with some XFCE plugins, it is quite easy to keep an eye on the system resources.

After we've downloaded the ISO file, we can burn it to a DVD or extract it to a USB stick...

Windows users can use the "Win32 Image writer" which you can download from `https://launchpad.net/win32-image-writer`. The program should be self-explanatory...

Linux and OSX users can use the console command `dd`:

```
dd if=/pfad/zum/kali-image.iso of=/dev/sdb bs=512k
```

This command must be executed as `root` or with `sudo`! But be careful with `dd`! This command doesn't forgive errors and can overwrite an entire hard drive without any security question!

With `if=` is the input file determined and with `of=` the output file. In my example, I have specified `/dev/sdb`, which is the device file of the second SCSI or SATA disk. This is also how the USB drives are addressed under Linux. It is important not to use for example `/dev/sdb1` because that would be the first partition on this disk, and we want to overwrite the entire disk including the partition table!

Under OSX this would be `/dev/disk1`. Here `/dev/disk1s0` would be the first partition and therefore wrong! The easiest way to identify the correct device file is to enter `df -h` in the terminal:

For example, if the output was

```
/dev/disk0s2   148Gi   86Gi   62Gi    58% ...
/dev/disk1s1   7.4Gi  5.2Gi  2.2Gi    71% ...
```

it is clear that the drive `disk1` with the 7.4 GB partition is the USB stick and `disk0` with a 148GB partition is the SSD of your computer. In this case `/dev/disk1` would be the output file.

The parameter `bs=512k` defines a block size of 512KB and can thus be adopted. `dd` does not report any progress and is not particularly fast either - make yourself a coffee, grab a snack or get some fresh air - you can count on 10 to 20 minutes.

Before doing this, the drive may have to be unmounted - this is done with:

`umount /dev/sdb1` (Linux)
`diskutil umount /dev/disk1s1` (OSX)

The unmounting have to be done via `sudo` or as `root`! As soon as `dd` has done its job the program informs you with a message like that:

```
5345+1 records in
5345+1 records out
2802616968 bytes transferred in 668.849633 secs (4190204 bytes/sec)
```

The computer can then get booted from the installation stick. Here you have the option of starting Kali from the USB stick and testing it without installation. This option is also very helpful if one of your systems no longer boots - so you can at least make a backup of your data with Kali and then investigate what caused that issue.

Like all Linux distros, Kali doesn't need much resources and runs smoothly on my Atom netbook with 2 GB of RAM - just 1 - 1.5% of the CPU power is required when idling. Therefore, I can recommend anyone interested of a VM to install Kali on an old notebook or netbook!

The Kali computer should have a sufficiently large hard drive or SSD! If you work with word lists or rainbow tables, you will quickly have to deal with file-sizes of 100GB and more... 500GB or more of disk space would be my recommendation.

I will go through the graphical installation with you at this point. As soon as you have selected the graphical installer from the boot menu, you will get to the installation wizard.

Here you first need to select your desired language and then click on the `Continue` button.

You may then be asked whether the installation should continue in your selected language. Depending on the version of the installation wizard, some texts may not have been fully translated - in such a case, part of the installation will be displayed in English. Select `Yes` and then click the `Next` button.

In the next step, select your country and click on `Next` again.

Then you will be asked for the keyboard layout... Select your keyboard layout and go to the next step.

Hardware detection is now carried out. This can take a minute or two. As soon as this is done, you will be asked for the computer name - I assign here `kali.local`. But you can let your creativity run free here. The `.local` at the end of the name assign the computer to the `.local` domain.

As soon as this is done, we have to assign a password for the user `root`. This user is the administrator on Linux and Unix systems and has the highest user rights. Normally you don't work directly as `root`, but for some of the things we'll do in this book, such as forging or intercepting packets and providing server services, it's easier to work directly as `root`.

The next step is partitioning - the most important from my point of view. Here we select Manual and create the following partition scheme for a computer with Legacy BIOS mode:

Mountpoint	Size	Format als
`/`	40-60GB	ext4
`/root`	40-100GB	ext4
---	4-8GB	swap
`/home`	all space which is left	ext4

For a newer computer with UEFI I recommend the following partition layout:

Mountpoint	Size	Format als
/boot/efi	2-4GB	fat32
/	40-60GB	ext4
/root	40-100GB	ext4
---	4-8GB	swap
/home	all space which is left	ext4

Further, the GUID partition table must also be used on a computer with UEFI.

Splitting up a drive that way makes sense because programs that run as `root` or a normal user store data in the respective user directory and they have so sufficient space, and there is still no risk that a program fills up the disk undetected which would cause the system having problems when booting and during the operation.

You can also format the system partition (`/`) without hesitation when reinstalling the system and the user data is safe on the partitions for `/root` or `/home`.

After we have finished creating the partitions, we are asked again whether we want to write the changes to the hard disk... We confirm this with `Yes` and the installation of the system begins.

This will be done after a few minutes and we will be asked if we want to install additional packages from a "network mirror". We should answer `yes` to this.

In the next step, we can configure a proxy server - usually, you will not need a proxy in your network to access the Internet - if you do, you can enter all informations in the specified format.

Click on `Next` and the missing software components and drivers will be automatically downloaded and installed from the internet.

After this, the GRUB bootloader is installed and set up... In a system with legacy support, you will be asked whether GRUB should be installed in the master boot record, or MBR for short - answer `Yes` and select the system disk in the next step.

The installation will then be completed and you can restart the system with a final click on the `Next` button when the installation is complete.

After restarting we can log in with the username and the password that was previously assigned.

If you are working with Linux for the first time, I strongly recommend reading a good book about Linux. Since Kali is based on Debian or Ubuntu, you should read books about one of the two distributions! Other Linux distributions can, for example, use different tools or sometimes rename configuration files differently or store them in different locations in the system. These are only details and not a problem for an experienced Linux user. A beginner should familiarize himself with his distro at the beginning.

A complete introduction to Linux at this point would go beyond the scope of the book. Also, I strongly assume that many readers will be familiar with Linux by now. I can warmly recommend the book "Hacking with Kali-Linux" (ISBN 978-3752686265) by my co-author Mark B. to everyone else.

Setup of the XFCE desktop environment

Next ,I want to show you how we set up our XFCE desktop. When you log in for the first time, you will be asked whether you want to start with empty bars or the default settings. At this point select the standard settings.

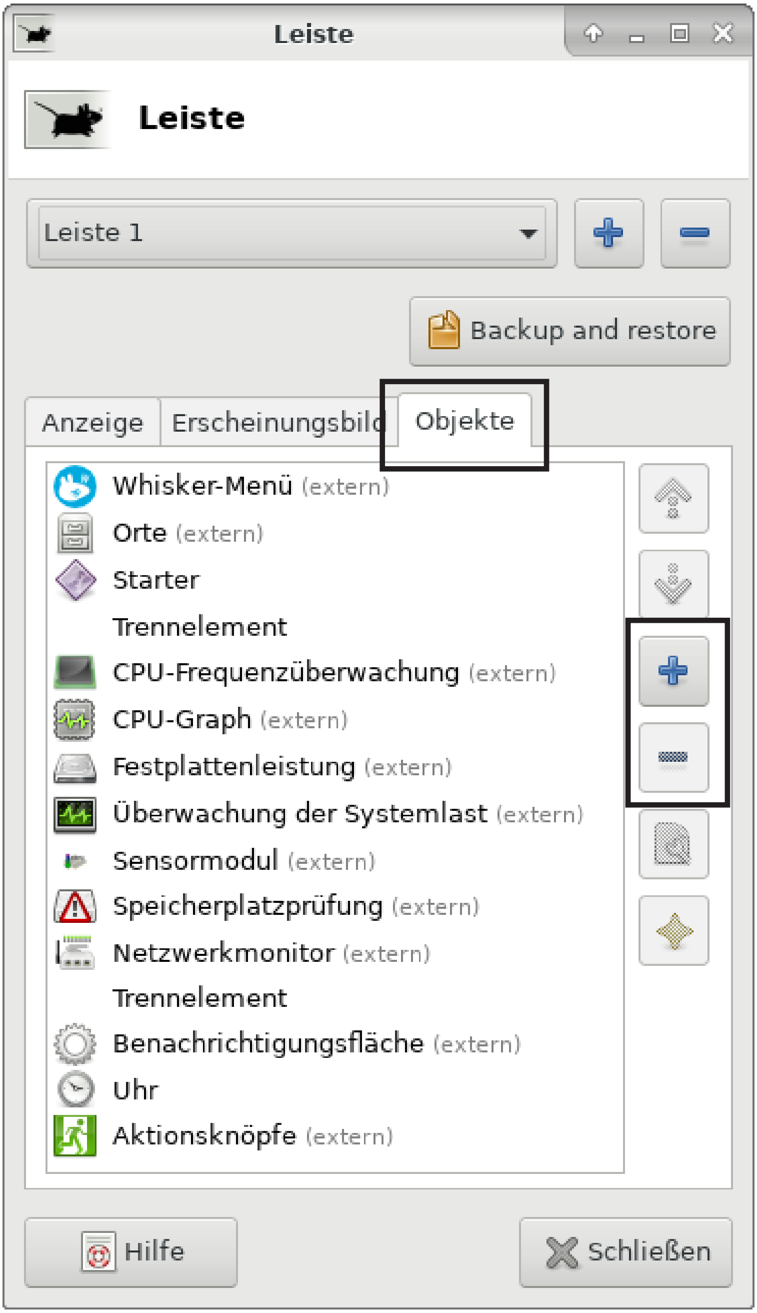
After a few moments, you will see your desktop with 2 bars (one above and one below). Before we set up the bars, we need a few XFCE plugins that we have to install in advance. To do this, we open a terminal - either via the command line icon in the lower bar or from the application menu at the top left. Then we run the two commands highlighted in bold:

```
root@kali:~# apt-get update
Holen:1 http://packages.microsoft.com/repos/vscode stable InRelease [2.802 B]
... Output shortend
Holen:6 http://archive-3.kali.org/kali kali-rolling/contrib amd64 Packages [101 kB]
Es wurden 16,4 MB in 3 s geholt (5.981 kB/s).
Paketlisten werden gelesen... Fertig
root@kali:~# apt-get -y install xfce4-*-plugin
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Hinweis: »xfce4-pulseaudio-plugin« wird für das Suchmuster »xfce4-*-plugin« gewählt.
Hinweis: »xfce4-systemload-plugin« wird für das Suchmuster »xfce4-*-plugin« gewählt.
... Output shortend
ayatana-indicator-application (0.5.2-1) wird eingerichtet ...
Trigger für libc-bin (2.27-3) werden verarbeitet ...
```

By the way, this mechanism is called package management and offers a very convenient way of downloading and installing software. As you can see, wildcard characters such as `*` allow you to install all XFCE4 plugins at once. You will now receive a list of all XFCE plugins that will be installed and the question of whether you want to continue - just confirm this with Enter and wait until everything has been installed. `apt-get` is the so-called package manager in Kali, with it programs, drivers and other system components can be installed, updated and uninstalled.

This means that all packages installed with it (fonts, drivers, system parts or user software) can be kept up to date with one and the same update mechanism. Incidentally, this is done with `apt-get update` followed by the command `apt-get upgrade`.

Now we can start to set up the panels:



Whisker-Menü (extern)
Orte (extern)
Starter
Trennelement
CPU-Frequenzüberwachung (extern)
CPU-Graph (extern)
Festplattenleistung (extern)
Überwachung der Systemlast (extern)
Sensormodul (extern)
Speicherplatzprüfung (extern)
Netzwerkmonitor (extern)
Trennelement
Benachrichtigungsfläche (extern)
Uhr
Aktionsknöpfe (extern)

Right-click the top bar and select `Panel` in the context menu and then in the submenu `Panel settings`.

Then select the `Objects` tab.

Then you can add elements with the `[+]` button or remove them with the `[-]` button to the right of the element list.

With the variety of programs at Kali, the `Whisker menu` is ideal, as it allows us to search directly for a program name.

The `Places menu` gives us quick access to the most important folders and a starter is like a program link.

All the monitoring plugins allow us to keep an eye on the system load and resource consumption.

The `notification area`, the `clock` and the `action buttons` with the logout and logout options have also been placed in the top bar on the far right. Practically, there is also a calendar hidden behind the clock that can be opened with one click.

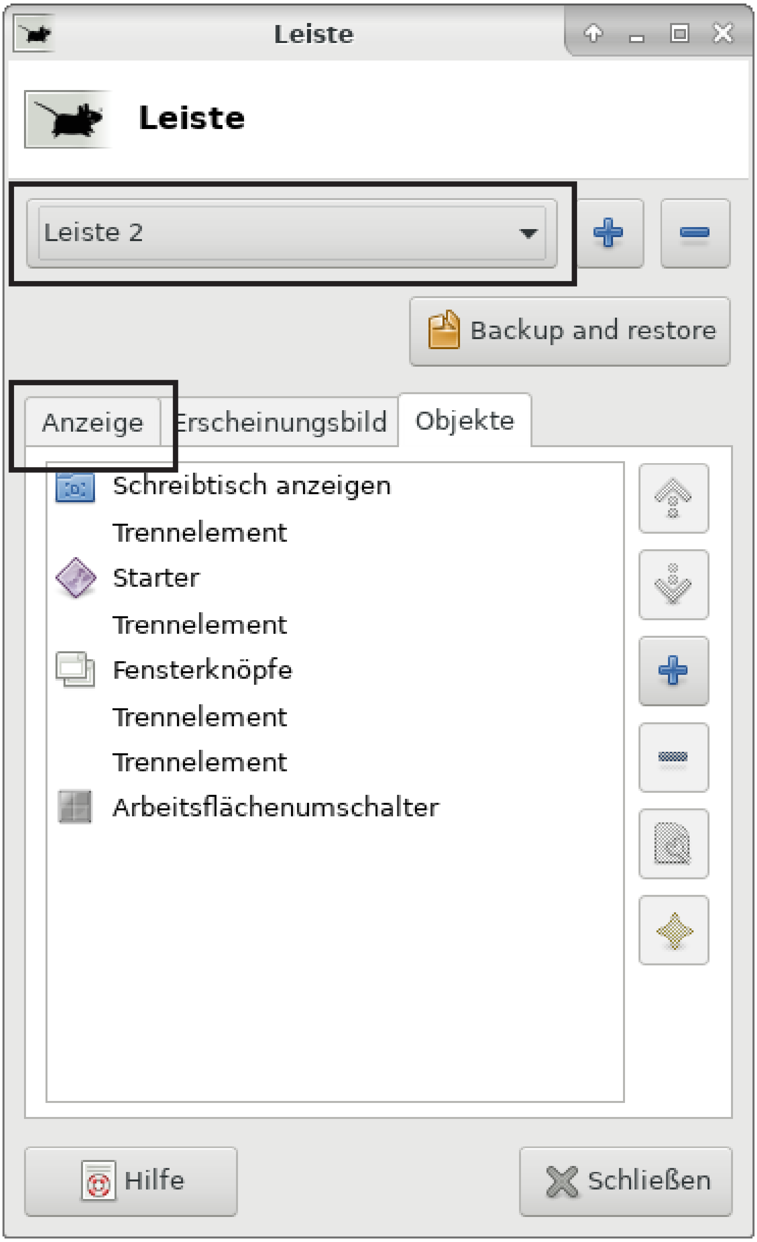
As soon as you have arranged the plugins and elements, you can switch to `Panel 2` (the lower bar) with the upper dropdown field.

The `window buttons` are buttons for switching between open windows and the `workspace switcher` allows you to switch between the virtual desktops.

After you have put the elements together according to your taste, you should also switch to the `Display` tab in the lower bar and readjust the line size and the length in %.

For the length, I would use 100% to stretch the bar across the width of the screen.

Once that's done, you can configure every single bar element.

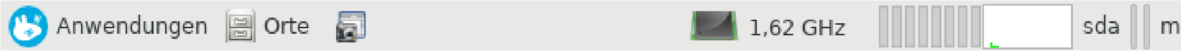


Leiste 2

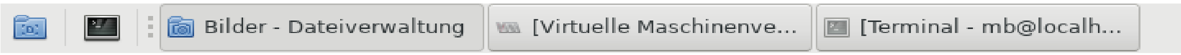
Schreibtisch anzeigen
Trennelement
Starter
Trennelement
Fensterknöpfe
Trennelement
Trennelement
Arbeitsflächenumschalter

To do this, click the element with the right mouse button and select `Properties` in the context menu.

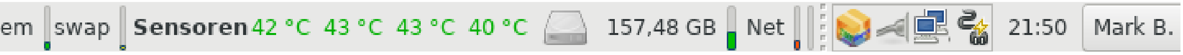
After a few basic settings, the top bar looks something like this:



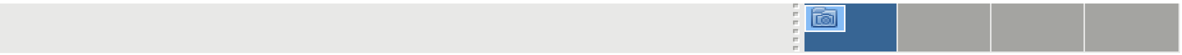
And the bottom bar like this:



If you are not familiar with the device names in Linux, then setting up the monitoring plug-ins is a good exercise for you!



em swap **Sensoren** 42 °C 43 °C 43 °C 40 °C 157,48 GB Net 21:50 Mark B.



INSTALLATION OF PYTHON 3, MODULES AND VS CODE

Installtion in Windows and Mac OSX

Windows- and Mac users can download an installer from the official website of Python: `https://www.python.org/downloads/`. After that just follow the steps in the installer.

Additional modules can be installed with a terminal command.

This command follows that scheme: `py.exe -[VERSION] -m pip install [PAKETNAME]` e.g.:

```
C:\Users\alicia> py.exe -3.6 -m pip install scapy
```

OSX-user need to write `pip3 install [PAKETNAME]` in the terminal - e.g.:
(The Terminal.app is located in the Programs folder in the subfolder Utils)

```
alicias-Mac-mini:~ alicia$ pip3 install scapy
```

Installation in Linux

Although Python version 3 is already preinstalled in Kali, `pip3` and `IDLE` are missing. Therefore I want to show you the installation on behalf of other Linux distros. Again we use the package manager. For this we need `root` rights:

```
kali@kali:~$ sudo apt-get install python3 python3-pip idle3
```

Further modules can be installed as `root` or normal user via terminal with the following command:

```
kali@kali:~$ pip3 install scapy
```

Installation and setup of Visual Studio Code

For Linux, programs are mostly distributed in the form of packages, and for Debian-based distributions such as Kali-Linux, the appropriate package format is `.deb`. So after we have downloaded the DEB file from `https://code.visualstudio.com/download` then we can open a terminal and switch to the downloads directory with the `cd` command and start the installation with `dpgk -i [PACKAGE NAME]`.

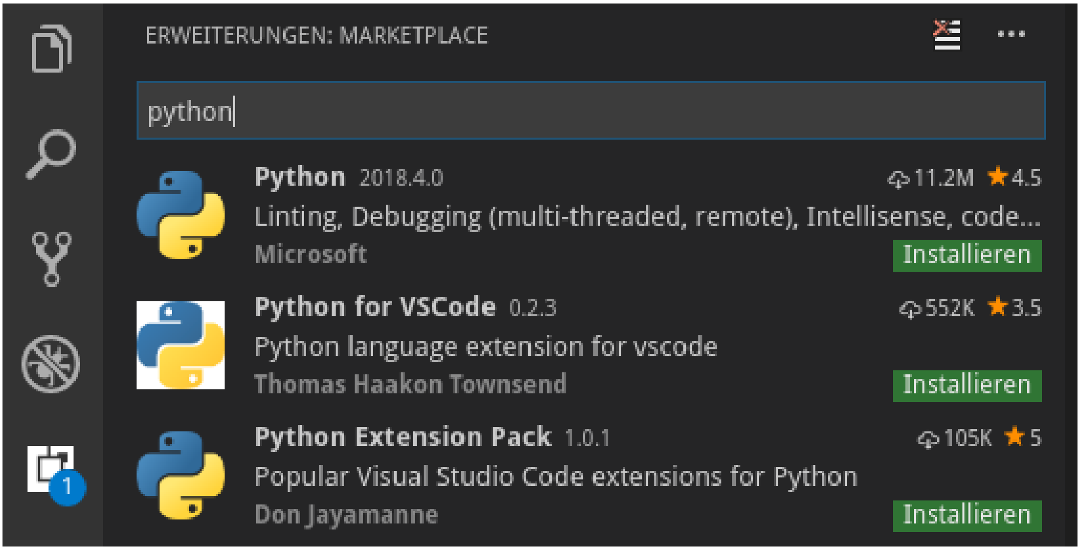
```
kali@kali:~$ cd Downloads/
kali@kali:~/Downloads$ sudo dpkg -i code_1.51.1-1605051630_amd64.deb
Selecting previously unselected package code.
(Reading database ... 308036 files and directories currently installed.)
Preparing to unpack code_1.51.1-1605051630_amd64.deb ...
Unpacking code (1.51.1-1605051630) ...
Setting up code (1.51.1-1605051630) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for shared-mime-info (1.15-1) ...
```

If the installation fails and you get an error that tells you some package is missing or some dependencies are not installed you can use the package-manager to fix that issue. With the following command you start the installation again and use the package manager (`apt`) to download and install the missing packages:

```
kali@kali:~/Downloads$ sudo apt --fix-broken install
```

As soon as the installation is finished we can start VS Code to install and set up the Python extension. To do this, open the applications menu and then the sub-menu "Development". This is where you should find VS Code.

After we start the program we should first install the Python extension from Microsoft. To do this, select the Marketplace symbol (bottom symbol) on the left side of the window.


ERWEITERUNGEN: MARKETPLACE

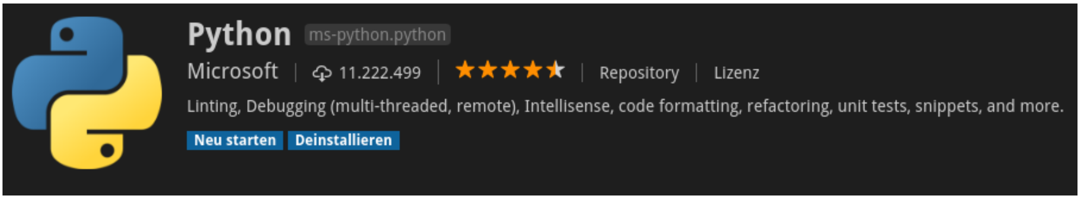
python

Python 2018.4.0 — 11.2M ★4.5
Linting, Debugging (multi-threaded, remote), Intellisense, code...
Microsoft

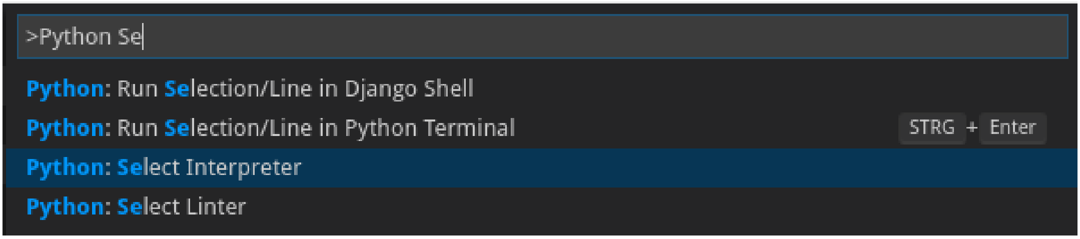
Python for VSCode 0.2.3 — 552K ★3.5
Python language extension for vscode
Thomas Haakon Townsend

Python Extension Pack 1.0.1 — 105K ★5
Popular Visual Studio Code extensions for Python
Don Jayamanne

Then you can enter `python` directly into the search field. As you can see, you are presented with several possible extensions. You are welcome to try the others, but I am using the original plug-in from Microsoft for this book (the developer is always shown under the short description). Click on the green Install button and restart VC Code when prompted.


Python ms-python.python
Microsoft | 11.222.499 | ★★★★★ | Repository | Lizenz
Linting, Debugging (multi-threaded, remote), Intellisense, code formatting, refactoring, unit tests, snippets, and more.

After the restart, we still have to select the interpreter. To do this, open the command palette with `Ctrl` + `Shift` + `P` and search for "`python se`" in the dialog box that opens.


>Python Se

Python: Run Selection/Line in Django Shell
Python: Run Selection/Line in Python Terminal — STRG + Enter
Python: Select Interpreter
Python: Select Linter