IT and Network Security
WiSe 2020/21

Preparation

Nils Aschenbruck

Leonhard Brüggemann, Alexander Tessmer, **Stefanie Thieme**

Till Zimmermann

Release 20.10.2020
Submission none

Virtual Machine

Before starting with the first exercise, you need to set up the virtual reference system that will be used throughout the course of this lecture. It is highly advised that you use this system as your development environment – not only because it provides certain features that are important for future exercises, but also because all your programs have to be executable on this system in order for you to receive any points.

Begin by downloading and installing *VirtualBox* [1] for your host system (Windows, Linux, ...). Proceed by downloading the official 64-bit *Kali Linux 2020.3*-Image [2][1]. Now set up the virtual machine (VM) by following the *VirtualBox* dialogue after you click *New*. We recommend that you allocate *at least* 2 GB RAM and 10 GB hard disk space.

On the first boot of your VM you will be asked to select an installation medium. Use the previously downloaded *Kali* image (.iso) and follow the installation instructions[2]. After this, you are ready to explore the functionalities of *Kali Linux* on your own!

Note: If you have used Kali Linux before, you will notice that they have changed their default user policy from *default root* to *default non-root* as of version 2020.1 [3]. During the exercises you will use and write tools that require both root and non-root access.

Having trouble logging in after you updated and upgraded your system? Do not worry! First: Congratulations, you are a user that is interested in keeping her software secure and up to date! Now you have two options: You can either deinstall *Virtualbox Guest Additions*[3] or select Kernel Version 5.7 instead of 5.8 in the *GRUB* menu.

[1] Choose the *Installer* – neither *Live*, nor anything else.
[2] selecting *top10* in the *Software Selection* dialogue suffices. Therefore, you can simply disable *default*.
[3] https://superuser.com/questions/1432429
You can tell if the Guest Additions were installed and find the right version using `lsmod | grep vboxguest` ; `/usr/sbin/VBoxClient --version`

Python 3

Now that you have learned the ropes of using Kali Linux, we can move on to the programming language that has to be used in all exercises: Python 3.8.5[4]! In addition to the default python modules, we will make use of *numpy*[5]. Install this package with *pip3*[6].

If you have no experience using python, you should make the most of the time until the first exercise is released (27.10.2020). Try starting with the introduction from the *Web Technologies* lecture [4] and search the web for more. The official python website's comprehensive tutorial is a good starting point [5].

Network Programming

As the title of this lecture suggests, networks play an important part. In order to assess their security vulnerabilities, a fair share of our time will be spent doing network programming. If you are not familiar with this or have not done this in python, you should take a look at the following exercise:

Imagine, you want to download a top-secret document from a password-protected file server. In order to obtain the password, you have to (correctly!) answer questions from a mysterious sphinx server. Of course, this is no appropriate security architecture, but a hopefully fun introduction to socket programming in python.

Write a python client that acquires the password, conforming to this "protocol" (see also figure 1):

1. First, greet the sphinx server with "Hello Sphinx!", otherwise you will be ignored.
2. Send your matriculation number.
3. If you have started the conversation successfully, the sphinx will ask you three questions. Answer them correctly to receive the password. Otherwise, your connection will be closed and you have to restart your client and begin anew. The sphinx does not judge you or your wrong answers.

Please note:

1. You can find the sphinx server at 131.173.33.211. It will log all communication for internal purposes.
2. Use TCP server port 4711.

[4] already included in Kali Linux 2020.3
[5] https://numpy.org/
[6] https://pkg.kali.org/pkg/python-pip

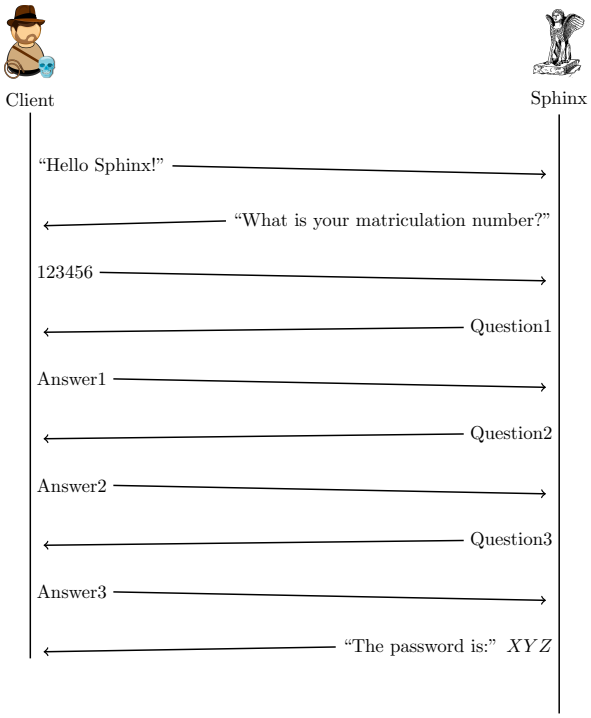


Figure 1: The sphinx protocol

3. All messages must be strings – even your matriculation number (e.g. *'123456'*).
4. The sphinx loves a nicely encoded string. Use *utf-8* to decode the mysteries!
5. Only the answers to the sphinx' questions are to be read from command line. Hard-code other messages and print them to screen before sending.
6. You can find information on python socket programming in [6] and a tutorial in [7].

Happy Coding!

References

[1] https://www.virtualbox.org/

[2] https://www.kali.org

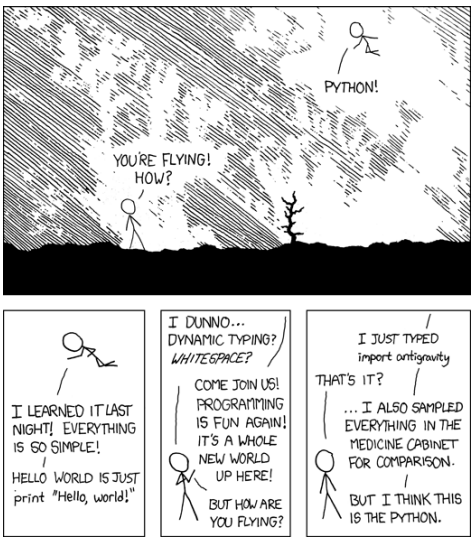
[3] https://www.kali.org/news/kali-default-non-root-user/

[4] https://www.youtube.com/watch?v=z4NlAzRpAj0

[5] https://docs.python.org/3/tutorial/

[6] *Socket Programming HOWTO*, https://docs.python.org/3/howto/sockets.html

[7] *Socket Programming in Python (Guide)*, https://realpython.com/python-sockets/



xkcd.com/353/