



IOT device network scanner

Installation manual

Bachelor in the IT-Factory
Keuzerichting Cloud and cyber security

Name: Simon Duchateau

Academic year 2020-2021

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

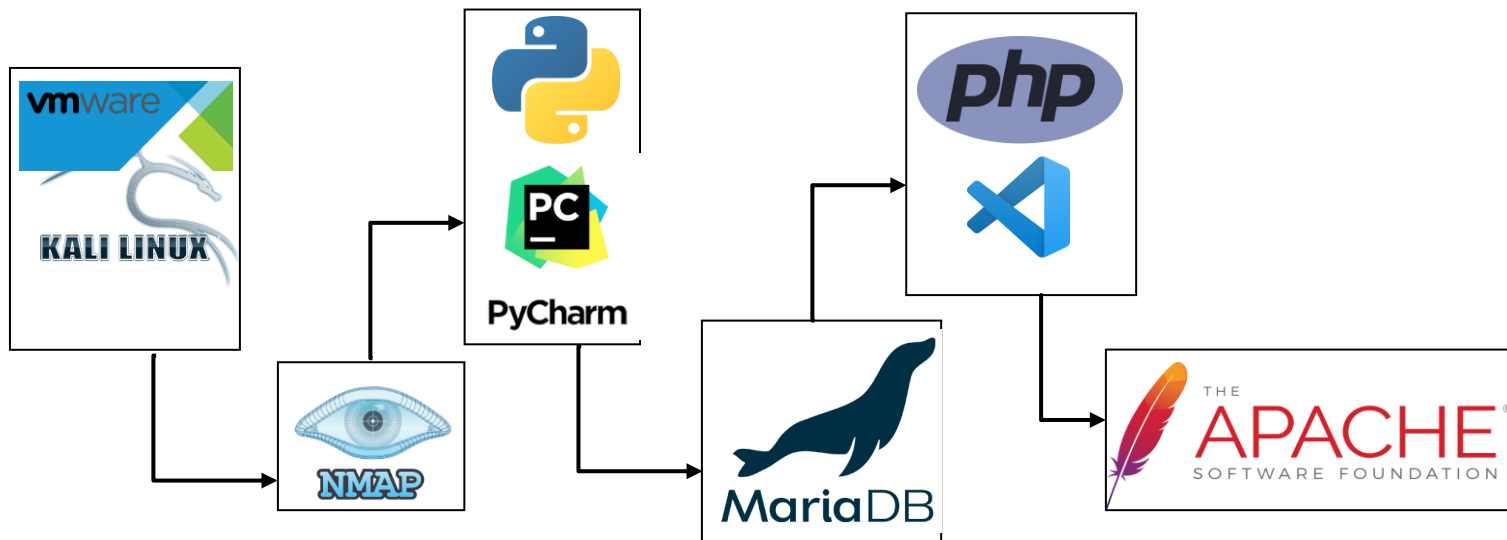
Table of content

1	INTRODUCTION	2
2	WHAT HAPPENS IN THE BACKGROUND?	4
3	CREATE VIRTUAL MACHINE IN VMWARE WORKSTATION	6
3.1	Select ISO file and Operating system	7
3.2	Virtual machine settings	7
3.3	Update Virtual machine.....	7
3.4	Install VMWare tools.....	8
4	INSTALL PYTHON	9
4.1	Install python	9
4.2	Install nmap for python	9
4.3	Install Pycharm.....	10
5	INSTALL MARIADB	11
6	INSTALL PHPMYADMIN	14
7	PHP PROJECT	15
8	CHECK IF EVERYTHING WORKS.....	16

1 INTRODUCTION

The past weeks I had the opportunity to create an application called the IOT Devices network scanner. You should use this application to check if there are unwanted devices or unwanted open ports on devices within your network. The focus of this application lays on IOT devices, IOT devices are devices that help you with your daily routines like a smart thermostat or smart light switches. Why did we focus on IOT devices? Because IOT device are not that rare anymore and if they are configured incorrectly could cause some serious network breaches.

Before I start explaining how to install the IOT device network scanner I would like to explain what we are using and how it works. We used a lot of tools and software to create but also to run this application.



The first thing you need is to install a Kali Linux virtual machine. I used Kali because I am familiar with this Linux distribution and it already has the basic scanning software installed. We used VMWare Workstation Pro. This virtual machine is the base of the whole project.

The scanning software we use is called nmap, this is an open source network scanner. We created a Python program using PyCharm that does the nmap network scan and pushes the result of the scan to a local database. You are not obligated to use Pycharm. MariaDB is the software that handles the storage of the information.

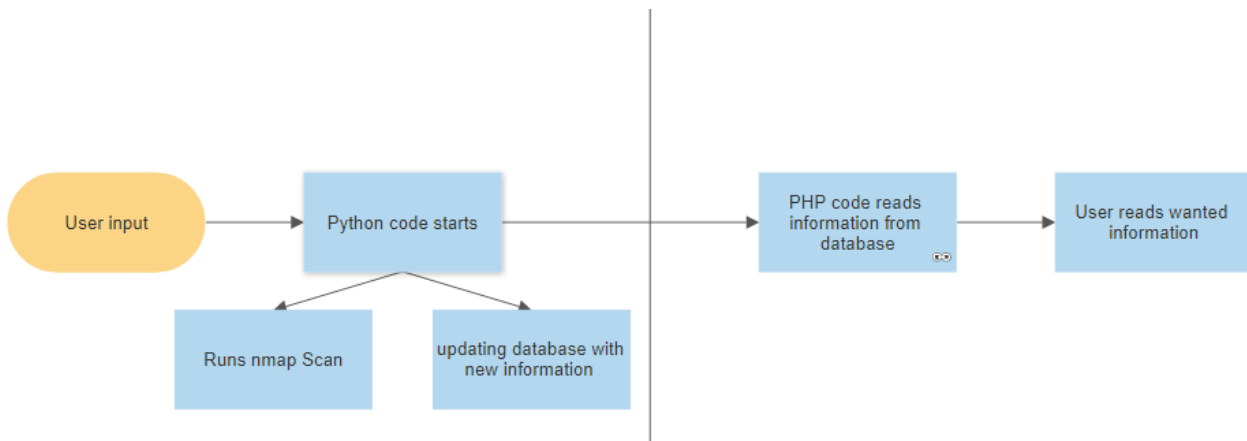
I used Visual Studio Code to create our front-end application and as coding language mainly PHP. If you want to use another PHP editor you are free to use your favorite one. This way we could easily connect to our database and retrieve data.

After we completed the project we wanted to make it visible for users. So we used the Apache web server software to publish the application. Optionally, you also can install PHPMyAdmin to monitor your database.

In this document I would like to explain how to install all the needed software correctly. I also would like to lead you through the configuration of these particular services. If all the packages are installed and configured correctly, I will explain step by step how you can install the application itself.

If you want to know how to use this application I would suggested reading the User manual. In this document I lead you step by step through every page and all the features of the application.

2 WHAT HAPPENS IN THE BACKGROUND?



1. The user starts the scan using the PHP application.

The screenshot shows the 'IOT device network scanner' web application. On the left is a sidebar menu with options: Dashboard, Result total scan, Result range scan, Search, Specific view, Upload Config, IOT Devices, Network Devices, Client devices, and Logout. The main content area displays a 'WELCOME ADMIN' message. Below this, there are two sections: 'Total scan' and 'Range scan'. The 'Total scan' section has an input field for '192.168.0.0' and a 'Start Scan' button. The 'Range scan' section has input fields for 'IP-Adres: 0.0.0.0' and 'Netmask: 24', along with a 'Start Scan' button.

2. When the user starts the scan he starts a python script in the background. This python script does a lot of tasks.
 - a. It connects to the database
 - b. Deletes all the tables that are created previously
 - c. Creates new necessary tables
 - d. Start an nmap scan with the given IP-address (and if range scan netmask)
 - e. Uploads new information to the correct tables

- 3. The PHP code now reads the new gathered information in the database and uses it to update the pages
- 4. User now has access to the new information in the user interface

IOT device network scanner

Dashboard

Result total scan

Devices

Ports

Result range scan

Search

Specific view

Upload Config

IOT Devices











































Network Devices

Client devices

Logout

WELCOME ADMIN

View Devices

Id	IP address	Mac address	Vendor	Operating System	
1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	  
2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  
3	192.168.0.4	D8:CB:8A:A1:B2:C3	Micro-star Intl	Microsoft Windows XP SP3	  
4	192.168.0.5	BC:60:A7:01:AD:2B	Sony Interactive Entertainment		  
5	192.168.0.6	B8:2C:A0:A1:B2:C3	Resideo	Sharp AR-C260M or AR-M351N printer	  
6	192.168.0.7	40:F5:20:D5:E6:F7	Espressif	ESP-IDF (ESP32, ESP32-S2)	  
7	192.168.0.8	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  
8	192.168.0.9	40:F5:20:D6:E7:F8	Espressif	ESP-IDF (ESP32, ESP32-S2)	  
9	192.168.0.10	D4:6A:6A:3C:6E:F2	Hon Hai Precision Ind.	VxWorks	  
10	192.168.0.11	40:F5:20:D7:E8:F9	Espressif	ESP-IDF (ESP32, ESP32-S2)	  
11	192.168.0.12	D8:CB:8A:A2:B3:C4	Micro-star Intl	Microsoft Windows XP SP3	  
12	192.168.0.13	D4:A6:51:A1:B2:C3	Tuya Smart	Tuya AIOT	  
13	192.168.0.14	F4:06:69:D3:86:DC	Intel Corporate	Linux 4.15 - 5.6	  
14	192.168.0.15	FC:FC:48:A1:B2:C3	Apple Inc.	Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0)	  

3 CREATE VIRTUAL MACHINE IN VMWARE WORKSTATION

For testing purposes I used an Virtual Machine. This way my configurations won't affect my local device. In this step I would like to explain how I created my virtual machine using VMware Workstation. I used VMware Workstation because I am more experienced with this software and I think it is easy to create and manage your virtual machines.

After creating a typical virtual machine it is time to choose an Operating System. This choice was rather obvious. I chose to use Kali Linux because Kali already had scanning software installed.

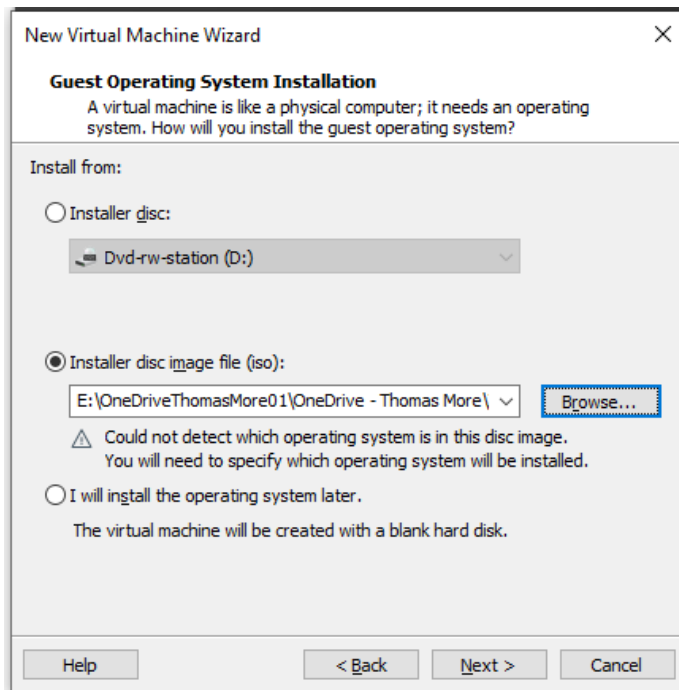
The settings of the virtual machine are decisions I made looking at the hardware I use on my local device. You can choose to use less Memory, Processors,... but this will affect the performance of you virtual machine. After the installation is finished it is very important to update your machine.

To get the New Virtual Machine Wizard you just need to click on the Create a New Virtual Machine on your home screen.



Click next

3.1 Select ISO file and Operating system



3.2 Virtual machine settings

Hardware Options	
Device	Summary
Memory	4.3 GB
Processors	2
Hard Disk (SCSI)	30 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

You can easily change these settings by right-clicking them and change them in what you prefer.

3.3 Update Virtual machine

Before we get to work we need to make sure our Virtual Machine is up-to-date. You can easily update you virtual machine by using these small commands.

```
Sudo apt update
```

```
Sudo apt upgrade -y
```


3.4 Install VMWare tools

If you want to use a shared folder or if you want to use full screen you need to install the VMware tools. You can install them by using this command. You just need to reboot the Virtual Machine after the installation.

```
(nemo9@nemo9) - [~]  
$ sudo apt-get -y install open-vm-tools-desktop fuse && reboot
```



4 INSTALL PYTHON

PyCharm

I needed to write a backend script that performs a nmap scan and uploads the data to a database. I chose to use Python as programming language because it makes it easy to implement the needed modules like nmap.

I used PyCharm as Python development environment because this tool is free to use and is compatible with Kali Linux. You need to make sure you open and install this tool as root user otherwise you are not able to run certain scripts.

4.1 Install python

```
(nemo9@nemo9)-[~/Desktop]
$ sudo apt-get install python3.9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3.9 is already the newest version (3.9.2-1).
python3.9 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

4.2 Install nmap for python

```
(nemo9@nemo9)-[~/Desktop]
$ sudo apt-get install python3-nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-5.10.0-kali3-amd64
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  python3-nmap
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 23.5 kB of archives.
After this operation, 100 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-nmap all 0.6.1-1.1 [23.5 kB]
Fetched 23.5 kB in 1s (33.4 kB/s)
Selecting previously unselected package python3-nmap.
(Reading database ... 280819 files and directories currently installed.)
Preparing to unpack .../python3-nmap_0.6.1-1.1_all.deb ...
Unpacking python3-nmap (0.6.1-1.1) ...
Setting up python3-nmap (0.6.1-1.1) ...
```

4.3 Install Pycharm

To install Pycharm you need to download the latest software package. You can find them here. Make sure you select the Linux version.

<https://www.jetbrains.com/pycharm/download/#section=linux>

1. After you downloaded this package you need to run following commands. Make sure you are in the correct directory.

```
(nemo9@nemo9)-[~/Downloads]
$ ls -al
total 511568
drwxr-xr-x  2 nemo9 nemo9      4096 Apr  1 10:08 .
drwxr-xr-x 16 nemo9 nemo9      4096 Apr  1 10:07 ..
-rw-r--r--  1 nemo9 nemo9 43603610 Mar 23 13:54 Nessus-8.13.1-debian6_amd64.deb
-rw-r--r--  1 nemo9 nemo9 480226082 Apr  1 10:08 pycharm-community-2020.3.5.tar.gz
```

2. After you downloaded the package you need to unzip the folder by using this command.
Sudo tar -xzf name of the package -C /opt

```
(nemo9@nemo9)-[~/Downloads]
$ sudo tar xzf pycharm-community-2020.3.5.tar.gz -C /opt
```

3. Change your directory by using following command.

Cd /opt/**name of the package**/bin

```
(nemo9@nemo9)-[~/Downloads]
$ cd /opt/pycharm-community-2020.3.5/bin
```

4. The installation is now completed you just need to run Pycharm by using following command.

./pycharm.sh

```
(nemo9@nemo9)-[/opt/pycharm-community-2020.3.5/bin]
$ ./pycharm.sh
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release
Apr 01, 2021 10:10:52 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
```

5 INSTALL MARIADB

After the scan is performed I need to make sure the data is stored in a database. Because I run the Kali Linux distribution I chose to use MariaDB. I had to choose between MariaDB and MySQL but MySQL isn't that compatible with Kali as MariaDB. If you follow these steps your installation will be quite easy.

<https://computingforgeeks.com/how-to-install-mariadb-on-kali-linux/>

1. We'll use the MariaDB apt repository for Debian 10 (Buster). Ensure you install the following software dependencies.

```
sudo apt -y install software-properties-common gnupg2
```

2. Add MariaDB APT repository to Kali Linux.

```
sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com
0xF1656F24C74CD1D8
echo "deb [arch=amd64]
http://mariadb.mirror.liquidtelecom.com/repo/10.5/debian buster main" |
sudo tee /etc/apt/sources.list.d/mariadb.list
```

3. Update your APT index before the actual installation of MariaDB on Kali Linux.

```
$ sudo apt update
Get:1 http://mariadb.mirror.liquidtelecom.com/repo/10.5/debian buster
InRelease [3,154 B]
Get:2 http://mariadb.mirror.liquidtelecom.com/repo/10.5/debian
buster/main amd64 Packages [28.0 kB]
Hit:3 http://kali.download/kali kali-rolling InRelease
Fetched 31.1 kB in 1s (29.4 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
839 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

4. After addition of the repository, we can install MariaDB server and client software packages on Kali Linux using the apt package manager.

```
sudo apt install mariadb-server mariadb-client
```

5. If you had mysql-common package installed, you may have to remove it.

```
sudo apt remove mysql-common
```

6. Hit the **y** key on the keyboard when prompted to begin installation.

```
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  galera-4 libdbd-mariadb-perl libdbi-perl libhtml-template-perl
  libreadline5 libterm-readkey-perl mariadb-client-10.5
  mariadb-client-core-10.5 mariadb-common mariadb-server-10.5
  mariadb-server-core-10.5 rsync
Suggested packages:
  libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl
  libipc-sharedcache-perl mailx mariadb-test netcat-openbsd
The following NEW packages will be installed:
  galera-4 libdbd-mariadb-perl libdbi-perl libhtml-template-perl
  libreadline5 libterm-readkey-perl mariadb-client mariadb-client-10.5
  mariadb-client-core-10.5 mariadb-server mariadb-server-10.5
  mariadb-server-core-10.5 rsync
The following packages will be upgraded:
  mariadb-common
1 upgraded, 13 newly installed, 0 to remove and 130 not upgraded.
Need to get 27.3 MB of archives.
After this operation, 217 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
....
```

7. Start and enable mariadb service after installation.

```
sudo systemctl enable --now mariadb
```

8. Confirm the service is started.

```
$ systemctl status mariadb
130 x
• mariadb.service - MariaDB 10.5.8 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled;
   vendor preset: disabled)
   Drop-In: /etc/systemd/system/mariadb.service.d
            └─migrated-from-my.cnf-settings.conf
   Active: active (running) since Fri 2021-01-22 14:18:15 EST; 19s
   ago
     Docs: man:mariabdb(8)
           https://mariadb.com/kb/en/library/systemd/
  Main PID: 7012 (mariabdb)
    Status: "Taking your SQL requests now..."
     Tasks: 15 (limit: 2274)
  Memory: 108.2M
       CPU: 482ms
    CGroup: /system.slice/mariadb.service
            └─7012 /usr/sbin/mariabdb
```

6 INSTALL PHPMYADMIN

I wanted a way to check my tables in my database. This is why I installed PHPMYAdmin. It is an easy service to install and use. Before you install PHPMYAdmin, you also need to install Apache. We also need the Apache services to host our PHP project.

<https://computingforgeeks.com/install-phpmyadmin-on-kali-linux/>

1. install PHP and Apache

```
(nemo9@nemo9) - [/etc]
$ sudo apt -y install wget php php-cgi php-mysql php-pear php-mbstring libapache2-mod-php php-common php-phpseclib php-mysql
```

2. Check state

```
(nemo9@nemo9) - [/etc]
$ php --version
PHP 7.4.15 (cli) (built: Feb 20 2021 09:45:56) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.15, Copyright (c), by Zend Technologies
```

3. Install PhpMyAdmin

```
(nemo9@nemo9) - [/etc]
$ sudo wget https://files.phpmyadmin.net/phpMyAdmin/5.0.4/phpMyAdmin-5.0.4-all-languages.tar.gz
[sudo] password for nemo9:
--2021-04-09 11:13:44-- https://files.phpmyadmin.net/phpMyAdmin/5.0.4/phpMyAdmin-5.0.4-all-languages.tar.gz
Resolving files.phpmyadmin.net (files.phpmyadmin.net)... 2a02:6ea0:c000::10, 2a02:6ea0:c000::6, 2a02:6ea0:c000::4, ...
Connecting to files.phpmyadmin.net (files.phpmyadmin.net)|2a02:6ea0:c000::10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12898226 (12M) [application/octet-stream]
Saving to: 'phpMyAdmin-5.0.4-all-languages.tar.gz'

phpMyAdmin-5.0.4-all-languages.tar.gz 100%[=====] 12.30M 22.5MB/s in 0.5s
2021-04-09 11:13:45 (22.5 MB/s) - 'phpMyAdmin-5.0.4-all-languages.tar.gz' saved [12898226/12898226]
```

4. Move the folder created from extraction to /usr/share/phpMyAdmin directory

```
(nemo9@nemo9) - [/etc]
$ sudo mv phpMyAdmin-* /usr/share/phpmyadmin
```

5. Create necessary folders with correct rights

```
(nemo9@nemo9) - [/etc]
$ sudo mkdir -p /var/lib/phpmyadmin/tmp

(nemo9@nemo9) - [/etc]
$ sudo chown -R www-data:www-data /var/lib/phpmyadmin

(nemo9@nemo9) - [/etc]
$ sudo mkdir /etc/phpmyadmin/
```



7 PHP PROJECT

This is a last step of the installation manual. In this step you need to install the PHP project itself. You already have the Apache service running you only need to download the PHP project and place it in the correct directory.

1. Run Visual studio code as root

```
(nemo9@nemo9) - [~/Desktop/Script]
$ sudo code --user-data-dir=~/.vscode-root"
```

2. Apache directory

```
(nemo9@nemo9) - [/var/www/html]
$ ls -al
total 40
drwxr-xr-x  7 root root 4096 May 17 12:55 .
drwxr-xr-x  3 root root 4096 Mar 12 13:30 ..
drwxr-xr-x 16 root root 4096 Apr 15 15:15 bower_components
drwxr-xr-x  2 root root 4096 Apr 15 15:15 config
drwxr-xr-x  4 root root 4096 Apr 15 15:15 dist
-rwxr-xr-x  1 root root   49 Apr 15 15:15 index.php
drwxr-xr-x  2 root root 4096 Apr 15 15:15 js
drwxr-xr-x  2 root root 4096 May 19 11:53 pages
-rwxrwxrwx  1 root root 3260 May 17 14:08 RangeScan.py
-rwxrwxrwx  1 root root 3204 May 17 14:19 TotalNetworkScan.py
```


8 CHECK IF EVERYTHING WORKS

The final step is to check if everything is working correctly. Opening your browser and searching for the IP-address of your Virtual Machine. If everything is configured correctly you should be able to access this page.

How to get the IP-address of the Virtual Machine? Open a new terminal on your Virtual machine and use following command. Your IP-address will be shown at the place of the red line.

```
(nemo9@nemo9) - [~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet XXXXXXXXXX netmask 255.255.255.0 broadcast XXXXXXXXXX
    inet6 2a02:1810:a520:7600:29e9:9e2b:9785:24f5 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe69:368f prefixlen 64 scopeid 0x20<link>
    inet6 2a02:1810:a520:7600:20c:29ff:fe69:368f prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:69:36:8f txqueuelen 1000 (Ethernet)
    RX packets 310 bytes 52486 (51.2 KiB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 113 bytes 82491 (80.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 36 bytes 2624 (2.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 2624 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Just open the your favorite browser and fill in the IP-address you get from previous step.

