

Cuckoo Installation Guide for Current Year

OS for Physical Machine is Windows 11, Installed VMware on top of that with Ubuntu 20.04, Installed KVM-QEMU and created a another Virtual Machine inside that again OS is Ubuntu 20.04

To install KVM/QEMU guide: <https://www.tecmint.com/install-kvm-on-ubuntu/>

Now that you are on KVM ubuntu machine open the terminal and fire the following commands

Step 1: We need to downgrade the python by setting Python 2 as the default python version as Cuckoo works with Python2

Firstly check the Host Machines especially the Host VM Internet Connection through browser Search

If not working good, try Command: `sudo dhclient`

This will turn on the internet for the VMs

```
$ sudo apt-get update
```

```
$ sudo apt-get upgrade
```

```
$ sudo apt install python2-minimal
```

```
$ python2 -V
```

Output: Python 2.7.18

```
$ ls /usr/bin/python*
```

```
$ sudo update-alternatives --install /usr/bin/python python /usr/bin/python2.7 2
```

```
$ sudo update-alternatives --install /usr/bin/python python /usr/bin/python3.5 3  
# If python3.5 3 in the above does not work try replacing it with 'python3...'
```

```
$ sudo update-alternatives --config python
```

```
$ sudo update-alternatives --config python
```

There are 2 choices for the alternative python (providing /usr/bin/python).

Selection	Path	Priority	Status
* 0	/usr/bin/python3.5	3	auto mode
1	/usr/bin/python2.7	2	manual mode
2	/usr/bin/python3.5	3	manual mode

Press <enter> to keep the current choice[*], or type selection number: 1 **#{Enter 1 of whichever index poiting to Python2.7 for you}**

```
$sudo apt install python2-pip
```

Installing Cuckoo directly does not come with a user interface such as a fancy dashboard

For that we take help of Anaconda

Go to anaconda.com and click on the download button for downloading anaconda for Linux based machine.

After the download, cut paste the anaconda file in the downloads to the Home folder in the File System.

Now get back to the terminal and follow the commands

```
$ sudo apt install libffi-dev libssl-dev libjpeg-dev zlib1g-dev swig
```

```
$ sudo apt install mongodb -y
```

```
$ sudo apt install postgresql libpq-dev -y
```

```
$ ls
```

you should be able to see the your Anaconda download with other folders

```
$ bash (AnacondaFilename with Extension Eg. Anaconda3-2023.03-1-Linux-x86_64.sh)
```

Press ENTER and then yes and then again yes

```
$ conda update conda
```

#if this gives you Conda command not found error try the below 4 commands or skip

```
$ export PATH=/home/anaconda3/bin:$PATH
```

```
$ echo 'export PATH=/path/to/anaconda3/bin:$PATH' >> ~/.bashrc
```

```
$ source .bashrc
```

```
$ conda update -all
```

```
$ conda update conda
```

```
#enter 'y'
```

```
$ conda update anaconda
```

#if this gives you anaconda command not found error try the below 4 commands or skip

```
$ conda install -c anaconda anaconda
```

then again try command : \$ conda update anaconda

```
$ pip2 install -U pip setuptools
```

```
$ anaconda-navigator
```

anaconda application window will open

- Click on the environment tab on the left hand side of the window
- Click on the plus sign at the bottom of the small window that opened
- This will lead to another small window asking for a environment name(give any name you wish Eg: cuckoosandbox) and python box checked(if there is a version choice in the dropdown select version 3.6 or leave it to default version)
- Click on create and you can see your environment getting created
- After the environment is created just click on the play button in front of the environment name and select open terminal
- And you will observe that a new window is popped open in your terminal. Therefore continue to enter the following command in the new terminal

```
$ pip2 install -U cuckoo
```

```
$ ls -la
# check in the list .cuckoo extension file exists or not
$ conda update -all
# press y and enter
$ cuckoo
#if no window opens
$ sudo nano ~/.cuckoo/conf/cuckoo.conf
$cuckoo web
# this will give away a error saying that the cuckoo web requires mongo db up and running. Then run the
below command
$ sudo nano ~/.cuckoo/conf/reporting.conf
# go down in the configuration editor to the mongodb part and edit the enabled= "yes" and now try again
$cuckoo web
# this will open the web based user interface for cuckoo sandbox
```

This the Secret to Cuckoo Sandbox installation for the year 2023. Go ahead upload the Malware Files and conduct analysis. Thank You.