



---

*CS6474: Software Testing Laboratory*  
*(Spring 2023)*

---

**Bishwajit Prasad Gond**  
**222CS3113**

Master of Technology  
222cs3113@nitrkl.ac.in

**Department of Computer Science & Engineering**  
**NIT, Rourkela**

April 11, 2023

# **CS6474 : Software Testing Laboratory 2023**

## **CUCKOO SANDBOX**

Prepared by  
BISHWAJIT PRASAD GOND  
222CS3113



# Contents

<b>1</b>	<b>Cuckoo Sandbox</b>	<b>1</b>
1.0.1	Tcases CMD command . . . . .	1
1.1	Command Explanation . . . . .	3
1.1.1	Sudo apt update . . . . .	3
1.1.2	Sudo apt upgrade . . . . .	3
1.1.3	sudo apt-get install python python-pip python-dev libffi-dev libssl-dev .	4
1.1.4	sudo apt-get install python-virtualenv python-setuptools . . . . .	4
1.1.5	sudo apt-get install libjpeg-dev zlib1g-dev swig . . . . .	4
1.1.6	sudo apt-get install mongodb . . . . .	4
1.1.7	sudo apt-get install postgresql libpq-dev . . . . .	4
1.1.8	sudo apt install virtualbox . . . . .	4
1.1.9	virtualbox . . . . .	4
1.1.10	Create vboxnet0 . . . . .	4
1.1.11	sudo apt-get install tcpdump apparmor-utils . . . . .	4
1.1.12	sudo usermod -a -G pcap cuckoo . . . . .	5
1.1.13	sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump . . . . .	5
1.1.14	getcap /usr/sbin/tcpdump . . . . .	5
1.1.15	sudo aa-disable /usr/sbin/tcpdump . . . . .	5
1.1.16	sudo pip install m2crypto . . . . .	5
1.1.17	sudo usermod -a -G vboxusers cuckoo . . . . .	5
1.1.18	cuckoo-setup-virtualenv.sh . . . . .	5
1.1.19	sudo -u cuckoo ./cuckoo-setup-virtualenv.sh . . . . .	5
1.1.20	source ~/.bashrc . . . . .	5
1.1.21	mkvirtualenv -p python2.7 cuckoo-test . . . . .	6
1.1.22	pip install -U pip setuptools . . . . .	6
1.1.23	pip install -U cuckoo . . . . .	6
1.1.24	wget https://cuckoo.sh/win7ultimate.iso . . . . .	6
1.1.25	ls -lah . . . . .	6
1.1.26	sudo mkdir /mnt/win7 . . . . .	6

1.1.27	sudo chown cuckoo:cuckoo /mnt/win7 . . . . .	6
1.1.28	sudo mount -o ro,loop win7ultimate.iso /mnt/win7 . . . . .	6
1.1.29	sudo apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage . . . . .	6
1.1.30	sudo apt-get -y install zlib1g-dev libjpeg-dev . . . . .	7
1.1.31	sudo apt-get -y install python-pip python-virtualenv python-setuptools swig . . . . .	7
1.1.32	pip install -U vmcloak . . . . .	7
1.1.33	vmcloak . . . . .	7
1.1.34	vmcloak-vboxnet0 . . . . .	7
1.1.35	vmcloak init -verbose -win7x64 win7x64base -cpus 2 -ramsize 2048 .	7
1.1.36	vmcloak clone win7x64base win7x64cuckoo . . . . .	7
1.1.37	vmcloak install win7x64cuckoo ie11 . . . . .	7
1.1.38	vmcloak snapshot -count 1 win7x64cuckoo 192.168.56.101 . . . . .	7
1.1.39	vmcloak list vms . . . . .	8
1.1.40	cuckoo init . . . . .	8
1.1.41	cd /.cuckoo/ . . . . .	8
1.1.42	ls . . . . .	8
1.1.43	cd conf/ . . . . .	8
1.1.44	ls . . . . .	8
1.1.45	cuckoo community . . . . .	8
1.1.46	nano virtualbox.conf . . . . .	8
1.1.47	make mode = gui . . . . .	8
1.1.48	while read -r vm ip; do cuckoo machine -add \$vm \$ip; done <<(vmcloak list vms) . . . . .	8
1.1.49	nano virtualbox.conf . . . . .	9
1.1.50	sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1 . . . . .	9
1.1.51	sudo sysctl -w net.ipv4.conf.eth0.forwarding=1 . . . . .	9
1.1.52	workon cuckoo-test . . . . .	9
1.1.53	cuckoo roter -sudo -group cuckoo . . . . .	9
1.1.54	nano routing.conf . . . . .	10
1.1.55	workon cuckoo-test . . . . .	10

1.1.56	cuckoo . . . . .	10
1.1.57	workon cuckoo-test . . . . .	10
1.1.58	cuckoo web -host 127.0.0.1 -port 8080 . . . . .	11

# 1 Cuckoo Sandbox

A Cuckoo Sandbox is a tool that is used to launch malware in a secure and isolated environment, the idea is the sandbox fools the malware into thinking it has infected a genuine host.

The sandbox will then record the activity of the malware and then generate a report on what the malware has attempted to do while in this secure environment.

These are great for security teams and malware analysts as they can be used to quickly gather IOC's which may be required for a security incident or a starting point for a piece of intel, it gives you quick and detailed information on how the malware is likely to behave.

Most commercial malware sandboxes are expensive, such as McAfee's enterprise version called Artemis. However Cuckoo is open source and free to download, and from my experience, the resulting output is almost identical.

Even though Cuckoo is free to download it can be quite complicated and time-consuming to set up for the first time, this is due to the Cuckoo requiring a number of dependencies, however once in place, it is an incredibly useful tool.

Once set up, Cuckoo is able to analyze many different malicious files (executables, office documents, pdf files, emails, malicious scripts) as well as malicious websites.

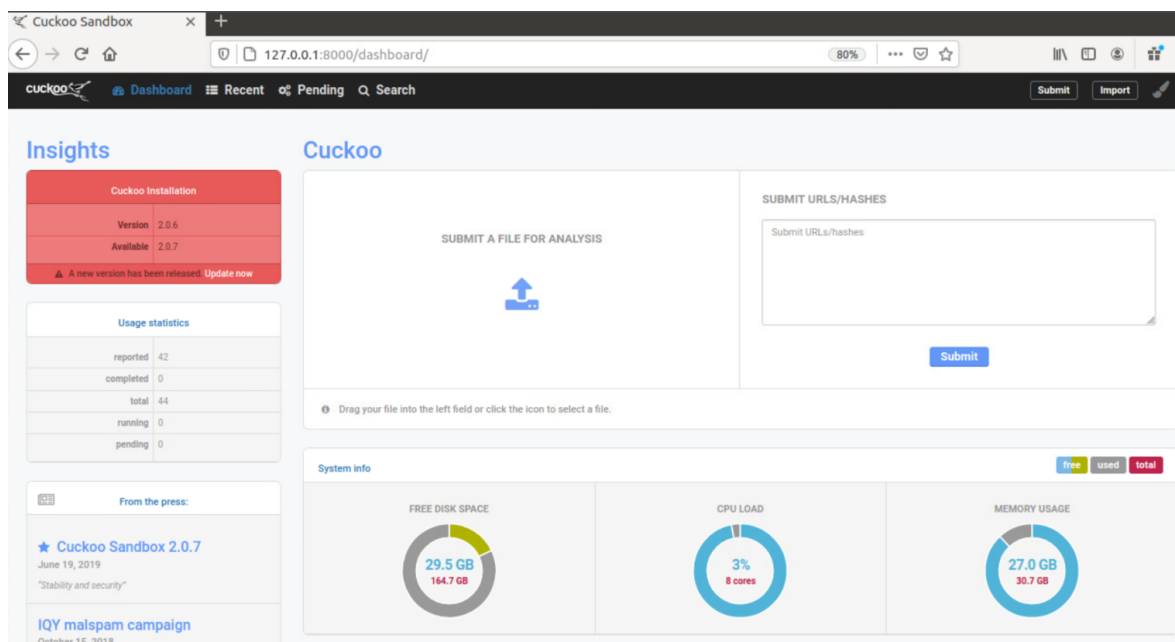


Figure 1: Cuckoo Sandbox Dashboard

## 1.0.1 Teases CMD command

```
1 Sudo apt update
2 Sudo apt upgrade
3 sudo apt-get install python python-pip python-dev libffi-dev
  libssl-dev
```

```

4  sudo apt-get install python-virtualenv python-setuptools
5  sudo apt-get install libjpeg-dev zlib1g-dev swig
6  sudo apt-get install mongodb
7  sudo apt-get install postgresql libpq-dev
8  sudo apt install virtualbox
9  open virtualbox
10 create vboxnet0
11 sudo apt-get install tcpdump apparmor-utils
12 sudo groupadd pcap
13 sudo usermod -a -G pcap cuckoo
14 sudo chgrp pcap /usr/sbin/tcpdump
15 sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
16 getcap /usr/sbin/tcpdump
17 sudo aa-disable /usr/sbin/tcpdump
18 sudo pip install m2crypto
19 sudo usermod -a -G vboxusers cuckoo
20 go to https://gist.github.com/jstrosch/
    de20131dda2aac5cd1116dd44b8f2474
21 chmod +x cuckoo-setup-virtualenv.sh
22 sudo u cuckoo ./cuckoo-setup-virtualenv.sh
23 source ~/.bashrc
24 mkvirtualenv p python2.7 cuckoo-test
25 pip install U pip setuptools
26 pip install U cuckoo
27 wget https://cuckoo.sh/win7ultimate.iso
28 ls lah
29 sudo mkdir /mnt/win7
30 sudo chown cuckoo:cuckoo /mnt/win7
31 sudo mount -o ro,loop win7ultimate.iso /mnt/win7
32 sudo apt-get -y install build-essential libssl-dev libffi-dev
33 python-dev genisoimage
34 sudo apt-get -y install zlib1g-dev libjpeg-dev
35 sudo apt-get -y install python-pip python-virtualenv python-
    setuptools swig
36 pip install U vmcloak
37 vmcloak
38 ** delete vboxnet from virtualbox **
39 vmcloak-vboxnet0
40 vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize
    2048
41 vmcloak clone win7x64base win7x64cuckoo
42 vmcloak install win7x64cuckoo ie11
43 vmcloak snapshot --count 1 win7x64cuckoo 192.168.56.101
44 vmcloak list vms
45 cuckoo init
46 cd ~/.cuckoo/
47 ls
48 cd conf/

```

```

49 ls
50 cuckoo community
51 nano virtualbox.conf
52 make mode = gui
53 while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(
    vmcloak list vms)
54 nano virtualbox.conf
55 delete cuckoo and its data
56 open new terminal
57 ip a
58 sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1
59     sudo sysctl -w net.ipv4.conf.eth0.forwarding=1
60 open new terminal
61 workon cuckoo-test
62 cuckoo roter --sudo --group cuckoo
63
64 nano routing.conf
65 change internet = eth0
66 nano reporting.conf
67 change mongodb enabled = yes
68 open new terminal
69 workon cuckoo-test
70 cuckoo
71
72 open new terminal
73 workon cuckoo-test
74 cuckoo web --host 127.0.0.1 --port 8080

```

open new terminal

## 1.1 Command Explanation

### 1.1.1 Sudo apt update

The sudo apt-get update command is used to download package information from all configured sources. The sources often defined in the /etc/apt/sources. list file and other files located in /etc/apt/sources.

### 1.1.2 Sudo apt upgrade

apt-get upgrade actually installs newer versions of the packages you have. After updating the lists, the package manager knows about available updates for the software you have installed.



### **1.1.3    `sudo apt-get install python python-pip python-dev libffi-dev libssl-dev`**

python python-pip python-dev libffi-dev libssl-dev software packages from the apt repositories are required to get Cuckoo to install and run properly.

### **1.1.4    `sudo apt-get install python-virtualenv python-setuptools`**

python-virtualenv python-setuptools are required to get cuckoo to install and run properly.

### **1.1.5    `sudo apt-get install libjpeg-dev zlib1g-dev swig`**

libjpeg-dev zlib1g-dev swig are required to get cuckoo to install and run properly.

### **1.1.6    `sudo apt-get install mongodb`**

Django-based Web Interface, MongoDB is required.

### **1.1.7    `sudo apt-get install postgresql libpq-dev`**

libpq is a set of library functions that allow client programs to pass queries to the PostgreSQL backend server and to receive the results of these queries.

### **1.1.8    `sudo apt install virtualbox`**

This command downloads and install virtual box with the newest version.

### **1.1.9    `virtualbox`**

This command is used to open the virtualbox.

### **1.1.10    `Create vboxnet0`**

This command is create a new host that is a gateway between host and guest.

### **1.1.11    `sudo apt-get install tcpdump apparmor-utils`**

This command installs the apparmor-utils. You need to install tcpdump in order to dump network traffic which occurs during analysis.

#### **1.1.12 sudo usermod -a -G pcap cuckoo**

The usermod command modifies the system account files to reflect the changes that are specified on the command line.

#### **1.1.13 sudo setcap cap\_net\_raw,cap\_net\_admin=eip /usr/sbin/tcpdump**

setcap sets the capabilities of each specified filename to the capabilities specified.

#### **1.1.14 getcap /usr/sbin/tcpdump**

getcap displays the name and capabilities of each specified file

#### **1.1.15 sudo aa-disable /usr/sbin/tcpdump**

aa-disable is used to disable one or more profiles. This command will unload the profile from the kernel and prevent the profile from being loaded on AppArmor startup

#### **1.1.16 sudo pip install m2crypto**

This command is used to install m2crypto.

#### **1.1.17 sudo usermod -a -G vboxusers cuckoo**

The usermod command modifies the system account files.

#### **1.1.18 cuckoo-setup-virtualenv.sh**

we are downloading sh file <https://gist.github.com/jstrosch/de20131dda2aac5cd1116dd44b8f2474>

#### **1.1.19 sudo -u cuckoo ./cuckoo-setup-virtualenv.sh**

The -u option allows you to run a command as the specified user name or user ID. So, you can run the command as a user other than the root.

#### **1.1.20 source ./bashrc**

For the changes to be applied, run the source command with the .bashrc file as an argument.

#### **1.1.21 mkvirtualenv -p python2.7 cuckoo-test**

This command is used for create new python environment for cuckoo.

#### **1.1.22 pip install -U pip setuptools**

Upgrade all packages to the newest available version of pip setuptools.

#### **1.1.23 pip install -U cuckoo**

Although the above, a global installation of Cuckoo in your OS works mostly fine, we highly recommend installing Cuckoo in a virtualenv.

#### **1.1.24 wget https://cuckoo.sh/win7ultimate.iso**

We are downloading virtaulbox win7ultimate.iso

#### **1.1.25 ls -lah**

List information about the FILEs (the current directory by default).

#### **1.1.26 sudo mkdir /mnt/win7**

Create the DIRECTORY, if they do not already exist.

#### **1.1.27 sudo chown cuckoo:cuckoo /mnt/win7**

These system calls change the owner and group of a file

#### **1.1.28 sudo mount -o ro,loop win7ultimate.iso /mnt/win7**

The mount options from command line will be appended to the list of op etc/fstab.tions from /  
The usual behavior is that the last option wins if there are more duplicated options.

#### **1.1.29 sudo apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage**

Before we install Cuckoo and VMCloak, the installation of multiple packages is required. These are dependencies VMCloak or Cuckoo require to function

#### **1.1.30 `sudo apt-get -y install zlib1g-dev libjpeg-dev`**

For the jpeg supports we want run above command.

#### **1.1.31 `sudo apt-get -y install python-pip python-virtualenv python-setuptools swig`**

Above command used for create the dependency between cuckoo and vmcloak.

#### **1.1.32 `pip install -U vmcloak`**

VMCloak only supports VirtualBox. Using this command install the vmcloak.

#### **1.1.33 `vmcloak`**

VMCloak is a utility for automatically creating Virtual Machines with Windows as guest Operating System. It has been tailored to generate Virtual Machines directly usable from within Cuckoo Sandbox, but it can also be used for other purposes as Cuckoo's components can be omitted through the configuration.

#### **1.1.34 `vmcloak-vboxnet0`**

This command create and start the vboxnet0 network.

#### **1.1.35 `vmcloak init -verbose -win7x64 win7x64base -cpus 2 -ramsize 2048`**

Create the VM and automatically install Windows. A Cuckoo analysis VM should have at least 2GB of memory and preferably two or more CPU cores.

#### **1.1.36 `vmcloak clone win7x64base win7x64cuckoo`**

This commands Creating cuckoo clone image form base file.

#### **1.1.37 `vmcloak install win7x64cuckoo ie11`**

This command is used for install internet explorer.

#### **1.1.38 `vmcloak snapshot -count 1 win7x64cuckoo 192.168.56.101`**

This command creating the snapshots of vms with ip address

#### **1.1.39 vmcloak list vms**

Listed the vm using above command.

#### **1.1.40 cuckoo init**

Creating the directory before use the cuckoo.

#### **1.1.41 cd /.cuckoo/**

This command is used to move to the cuckoo directory.

#### **1.1.42 ls**

After run above command it shows the list of directory content.

#### **1.1.43 cd conf/**

Here we can do some configurations the files.

#### **1.1.44 ls**

After run above command it shows the list of directory content.

#### **1.1.45 cuckoo community**

Install cuckoo community, which has useful signatures that will be useful while in analysis.

#### **1.1.46 nano virtualbox.conf**

We are using nano text editor to edit virtualbox.conf

#### **1.1.47 make mode = gui**

We are enabling GUI render for user friendly dashboard

#### **1.1.48 while read -r vm ip; do cuckoo machine --add \$vm \$ip; done <<(vmcloak list vms)**

Time to add the created VMs to Cuckoo. We will use the cuckoo machine `--add < vmname > < ip >` to tell Cuckoo to add the machine to its configuration. This has to be done for each machine, so let's make life easier and use vmcloak list vms.

### 1.1.49 nano virtualbox.conf

We are using nano text editor to edit virtualbox.conf

### 1.1.50 sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1

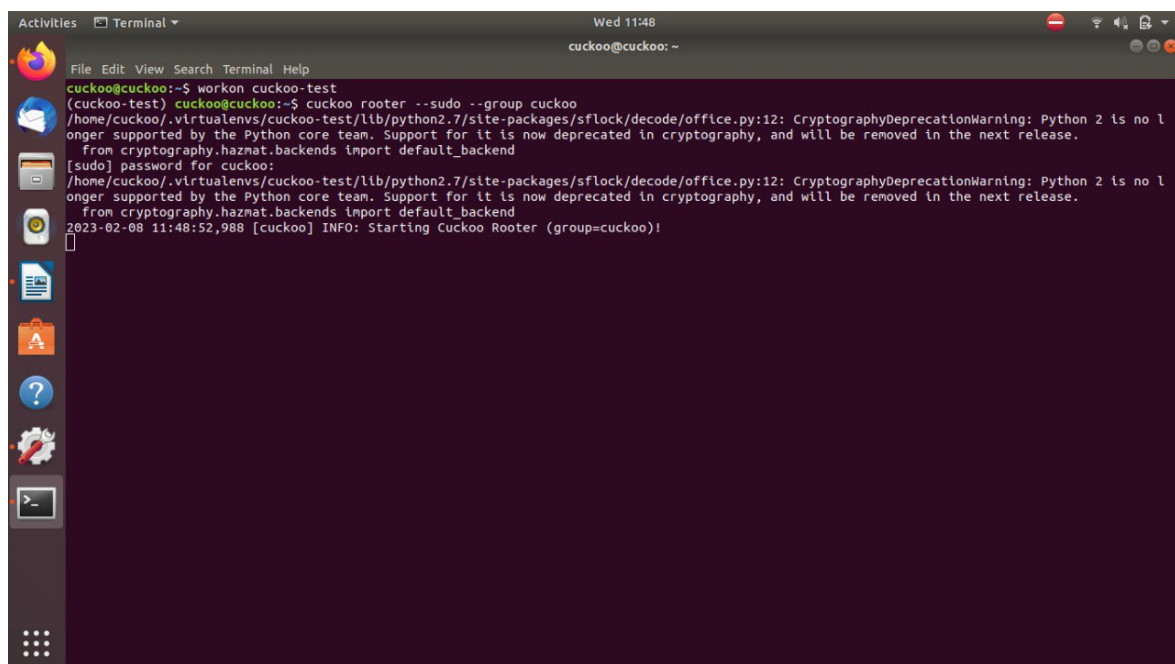
We are configuring virtualbox to allow ip forwarding.

### 1.1.51 sudo sysctl -w net.ipv4.conf.eth0.forwarding=1

We are configuring eth0 to allow ip forwarding.

### 1.1.52 workon cuckoo-test

This command is use to switch to cuckoo in virtual environment any further command in this environment will be executed in cuckoo-test.



```
Activities Terminal Wed 11:48
cuckoo@cuckoo: ~
File Edit View Search Terminal Help
cuckoo@cuckoo:~$ workon cuckoo-test
(cuckoo-test) cuckoo@cuckoo:~$ cuckoo rooter --sudo --group cuckoo
/home/cuckoo/.virtualenvs/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend
[sudo] password for cuckoo:
/home/cuckoo/.virtualenvs/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend
2023-02-08 11:48:52,988 [cuckoo] INFO: Starting Cuckoo Rooter (group=cuckoo)!
```

Figure 2: Screenshot of workon cuckoo-test

### 1.1.53 cuckoo rooter --sudo --group cuckoo

Since Cuckoo is installed in a virtualenv, and the Cuckoo user should not have root privileges, we can do the following from a root privileged user.

### 1.1.54 nano routing.conf

We are using nano text editor to edit routing.conf

**change internet = eth0**

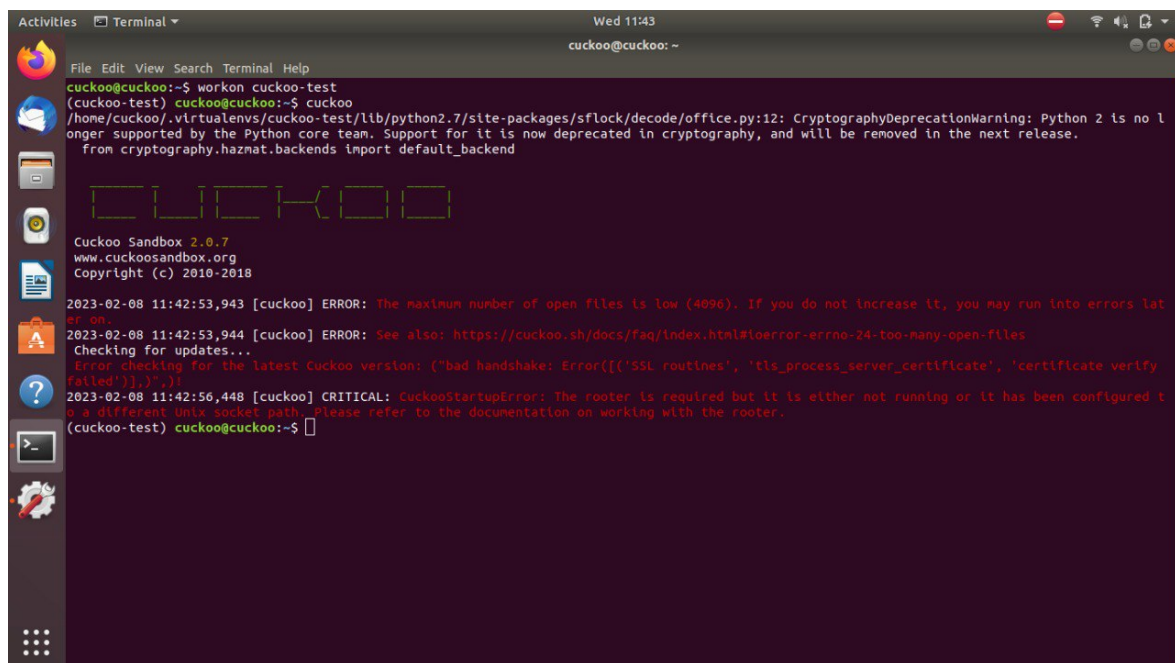
**nano reporting.conf**

**change mongodb enabled = yes**

Again we are opening new terminal for running the below command.

### 1.1.55 workon cuckoo-test

This command is use to switch to cuckoo in virtual environment any further command in this environment will be executed in cuckoo-test.



```
Activities Terminal Wed 11:43
cuckoo@cuckoo: ~
File Edit View Search Terminal Help
cuckoo@cuckoo:~$ workon cuckoo-test
(cuckoo-test) cuckoo@cuckoo:~$ cuckoo
/home/cuckoo/.virtualenvs/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend

Cuckoo
Cuckoo Sandbox 2.0.7
www.cuckoosandbox.org
Copyright (c) 2010-2018

2023-02-08 11:42:53,943 [cuckoo] ERROR: The maximum number of open files is low (4096). If you do not increase it, you may run into errors later on.
2023-02-08 11:42:53,944 [cuckoo] ERROR: See also: https://cuckoo.sh/docs/faq/index.html#ioerror-errno-24-too-many-open-files
Checking for updates...
Error checking for the latest Cuckoo version: ("bad handshake: Error([('SSL routines', 'tls_process_server_certificate', 'certificate verify failed')],)"),)
2023-02-08 11:42:56,448 [cuckoo] CRITICAL: CuckooStartupError: The router is required but it is either not running or it has been configured to a different Unix socket path. Please refer to the documentation on working with the router.
(cuckoo-test) cuckoo@cuckoo:~$
```

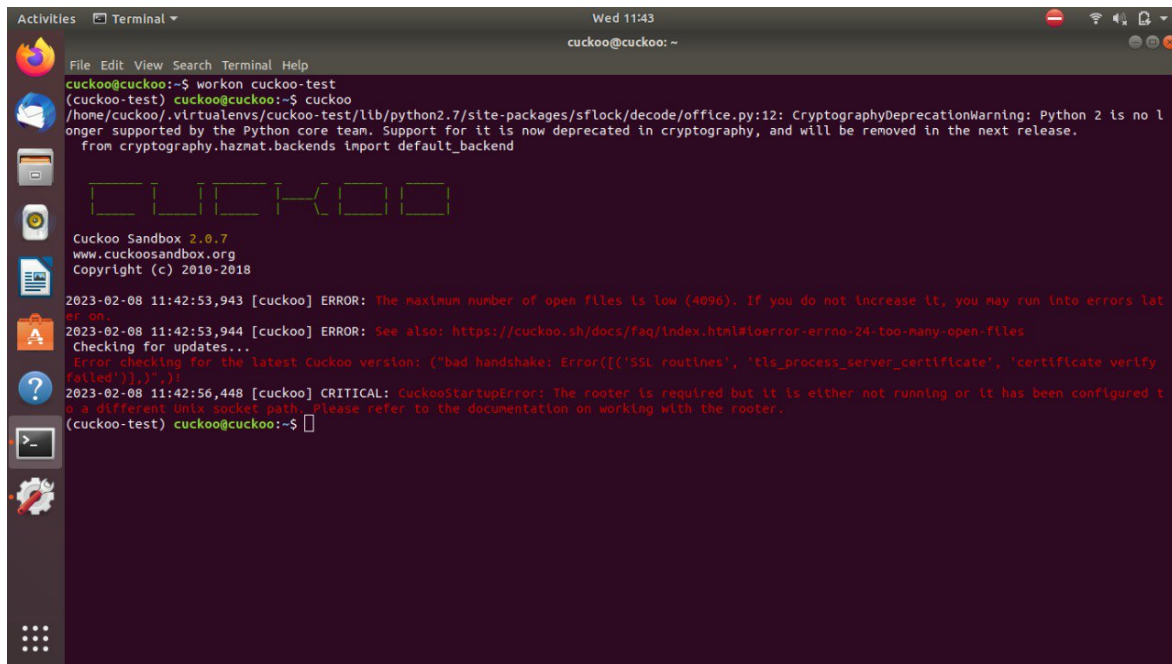
Figure 3: Screenshot of cuckoo

### 1.1.56 cuckoo

This Command is Used to start cuckoo program.

### 1.1.57 workon cuckoo-test

This command is use to switch to cuckoo in virtual environment any further command in this environment will be executed in cuckoo-test.



```
Activities Terminal Wed 11:43 cuckoo@cuckoo: ~
File Edit View Search Terminal Help
cuckoo@cuckoo:~$ workon cuckoo-test
(cuckoo-test) cuckoo@cuckoo:~$ cuckoo
/home/cuckoo/.virtualenvs/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend

  C U C K O O

Cuckoo Sandbox 2.0.7
www.cuckoosandbox.org
Copyright (c) 2010-2018

2023-02-08 11:42:53,943 [cuckoo] ERROR: The maximum number of open files is low (4096). If you do not increase it, you may run into errors later on.
2023-02-08 11:42:53,944 [cuckoo] ERROR: See also: https://cuckoo.sh/docs/faq/index.html#error-errno-24-too-many-open-files
Checking for updates...
Error checking for the latest Cuckoo version: ("bad handshake: Error([('SSL routines', 'tls_process_server_certificate', 'certificate verify failed')],)"), (-1,))
2023-02-08 11:42:56,448 [cuckoo] CRITICAL: CuckooStartupError: The router is required but it is either not running or it has been configured to a different unix socket path. Please refer to the documentation on working with the router.
(cuckoo-test) cuckoo@cuckoo:~$
```

Figure 4: Screenshot of workon cuckoo-test

### 1.1.58 cuckoo web -host 127.0.0.1 -port 8080

We are opening GUI based cuckoo dashboard on Internet Explorer on IP 127.0.0.1 port: 8080



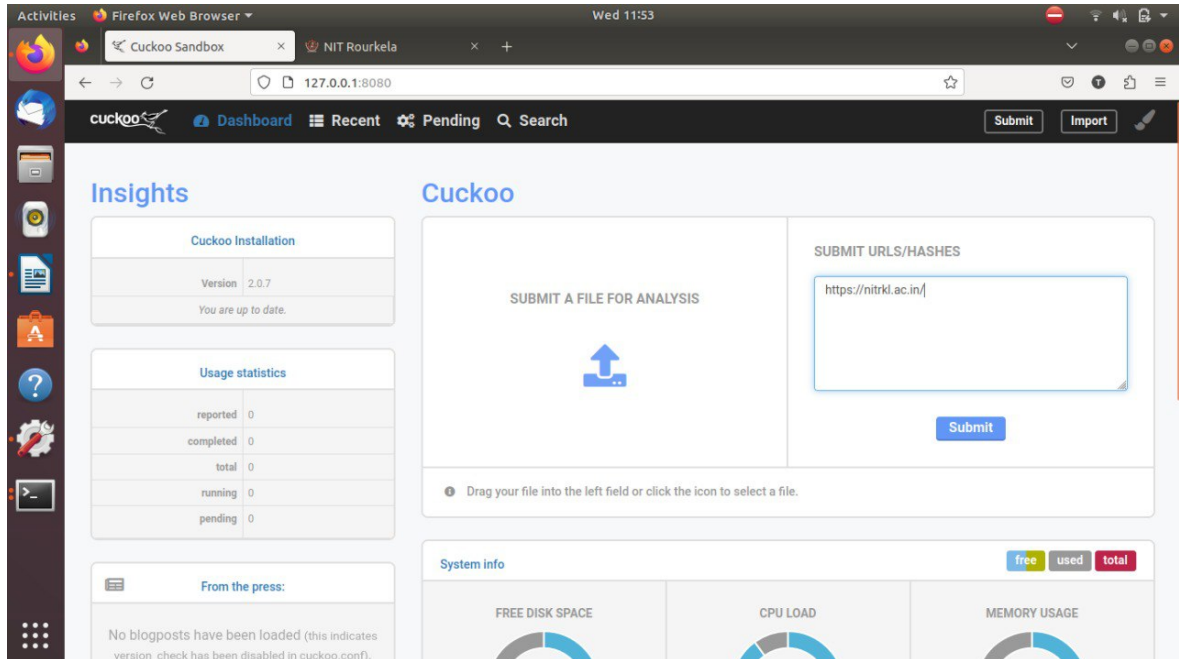


Figure 5: Screenshot of cuckoo dashboard

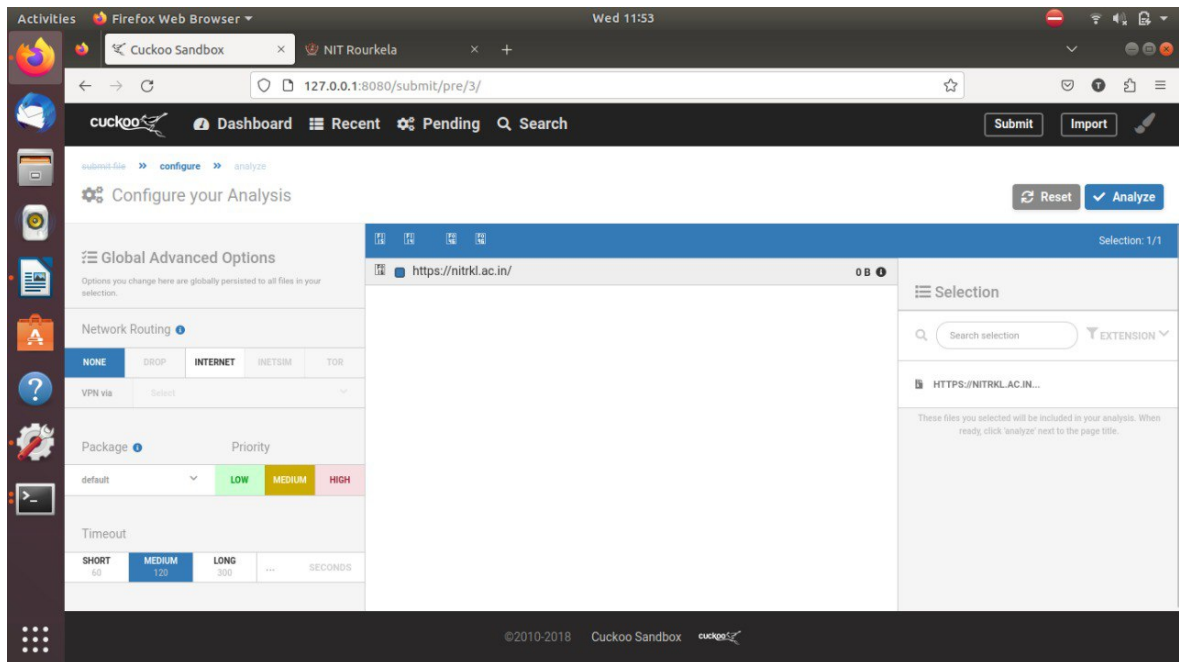


Figure 6: Screenshot of url injection using cuckoo