Cuckoo

Information Security Inc.

Contents

- What is Cuckoo?
- Cuckoo Testing Environment
- Cuckoo Installation (Guest OS)
- Cuckoo Installation
- Cuckoo: Web interface
- Cuckoo: Web interface and submitting files
- References

What is Cuckoo?

- Cuckoo is an open source automated malware analysis system.
- It's used to automatically run and analyze files and collect comprehensive analysis results that outline what the malware does while running inside an isolated Windows operating system

Cuckoo Testing Environment

- Host machine: Ubuntu Desktop 16.04.3 LTS
- Virtual environment: VirtualBox (5.1)

Cuckoo Installation

- Install VirtualBox

◎ Setup apt repository

```
deb http://download.virtualbox.org/virtualbox/debian xenial contrib
admin1@admin1-virtual-machine:/etc/apt$ pwd
/etc/apt
admin1@admin1-virtual-machine:/etc/apt$ cat sources.list
```

◎ Setup Oracle public key

```
admin1@admin1-virtual-machine:/etc/apt$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc
-O- | sudo apt-key add -
OK
admin1@admin1-virtual-machine:/etc/apt$ wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add
-
OK
```

◎ Install Oracle VirtualBox

```
sudo apt-get update
sudo apt-get install virtualbox-5.1
```

Cuckoo Installation

- Install Python, MongoDB (to use Django-based web interface)

```
sudo apt-get install python
sudo apt-get install mongodb
```

- Install ElasticSearch

```
add-apt-repository ppa:webupd8team/java
sudo add-apt-repository ppa:webupd8team/java
sudo wget -qO - https://packages.elasticsearch.org/GPG-KEY-elasticsearch | sudo apt-key add -
sudo add-apt-repository "deb http://packages.elasticsearch.org/elasticsearch/1.4/debian stable main"
sudo apt-get update
sudo  apt-get install oracle-java8-installer elasticsearch
sudo
Setting up java-wrappers (0.1.28) ...
sudo apt-get install elasticsearch
sudo update-rc.d elasticsearch defaults 95 10
sudo /etc/init.d/elasticsearch start
```

- Install SQLAlchemy and Python BSOn

```
sudo apt-get install python-sqlalchemy python-bson
```

Cuckoo Installation

- Install optional dependencies

```
sudo apt-get install python-dpkt python-jinja2 python-magic python-pymongo python-libvirt python-b
ottle python-pefile python-chardet swig libssl-dev clamav-daemon python-geoip geoip-database mono-utils
```

- For faster generation of PDF reports install wkhtmltopdf

```
sudo apt-get install wkhtmltopdf xvfb xfonts-100dpi
```

- If Pip is not installed, install Pip

```
sudo apt-get install python-pip
```

- Install Cybox and Maec

```
sudo pip install cybox==2.1.0.9
sudo pip install maec==4.1.0.11
```

Cuckoo Installation

- Install YARA

```
wget https://github.com/VirusTotal/yara/archive/v3.6.3.tar.gz
tar -zxf v3.6.3.tar.gz
cd yara-3.6.3/
sudo apt-get install automake libtool make gcc
./bootstrap.sh
```

- Compile YARA with Cuckoo module

```
sudo apt-get install libjansson-dev
./configure --enable-cuckoo
make
sudo make install
```

- Run the test cases to make sure everything is fine

```
============================================================
Testsuite summary for yara 3.6.3
============================================================
# TOTAL: 6
# PASS:  6
# SKIP:  0
# XFAIL: 0
# FAIL:  0
# XPASS: 0
# ERROR: 0
============================================================
make[3]: Leaving directory '/home/admin1/yara-3.6.3'
make[2]: Leaving directory '/home/admin1/yara-3.6.3'
make[1]: Leaving directory '/home/admin1/yara-3.6.3'
admin1@admin1-virtual-machine:~/yara-3.6.3$ make check
```

Cuckoo Installation

- Install pydeep

```
sudo apt-get install python-dev libfuzzy-dev
sudo git clone https://github.com/kbandla/pydeep.git
cd pydeep/
sudo python setup.py build
sudo python setup.py test
sudo python setup.py install
```

- Install tcpdump (installed by default in Ubuntu)
- Tcpdump requires root privileges, but since Cuckoo does not need to run as root set specific Linux capabilities to the binary

```
admin1@admin1-virtual-machine:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
admin1@admin1-virtual-machine:~$ getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

Cuckoo Installation

- Optional: Install Volatility

```
sudo apt-get install pcregrep libpcre++-dev python-dev -y
sudo apt-get install python-distorm3 python-pycryptopp python-openpyxl python-ujson -y
sudo pip install pycrypto
git clone https://github.com/volatilityfoundation/volatility.git
cd volatility/
sudo python setup.py build
sudo python setup.py install
```

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ pwd
/home/admin1/.cuckoo/conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ ls
auxiliary.conf  cuckoo.conf  kvm.conf     physical.conf    qemu.conf       routing.conf     vmware.conf   xenserver.conf
avd.conf        esx.conf     memory.conf  processing.conf  reporting.conf  virtualbox.conf  vsphere.conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ grep -i vola --color processing.conf  -A 3
# then be analyzed using Volatility to locate interesting events that can be
# extracted from memory.
enabled = yes
```

Cuckoo Installation

- Optional: Create a new user

```
admin1@admin1-virtual-machine:~$ sudo adduser cuckoo
Adding user `cuckoo' ...
Adding new group `cuckoo' (1001) ...
Adding new user `cuckoo' (1001) with group `cuckoo' ...
Creating home directory `/home/cuckoo' ...
Copying files from `/etc/skel' ...
```

- If using VirtualBox add the new user to the vboxusers group

```
sudo usermod -a -G vboxusers cuckoo
```

- Install Cuckoo

```
sudo apt-get install python-dev
sudo apt-get install libjpeg8-dev
sudo ln -s /usr/lib/x86_64-linux-gnu/libjpeg.so /usr/lib
pip install pillow
```

```
sudo apt install virtualenv
virtualenv venv
. venv/bin/activate
pip install -U pip setuptools
pip install -U cuckoo
```

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo$ cuckoo community
[cuckoo.apps.apps] INFO: Downloading.. https://github.com/cuckoosandbox/community/archive/master.tar.gz
[cuckoo] INFO: Finished fetching & extracting the community files!
```

Cuckoo Installation

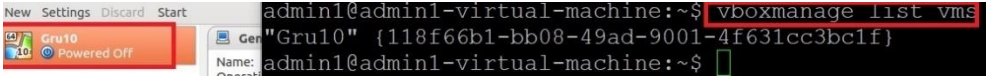
- Run Cuckoo

```
(venv) admin1@admin1-virtual-machine:~$ cuckoo

Cuckoo Sandbox 2.0.3
www.cuckoosandbox.org
Copyright (c) 2010-2017

Welcome to Cuckoo Sandbox, this appears to be your first run!
We will now set you up with our default configuration.
You will be able to see and modify the Cuckoo configuration,
Yara rules, Cuckoo Signatures, and much more to your likings
by exploring the /home/admin1/.cuckoo directory.

Among other configurable items of most interest is the
new location for your Cuckoo configuration:
/home/admin1/.cuckoo/conf

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).
```

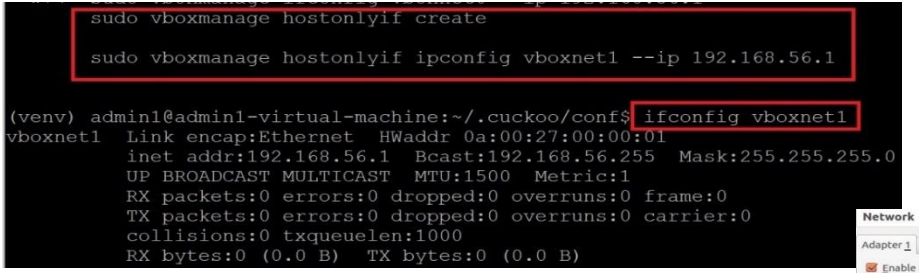
Cuckoo Installation (Guest OS)

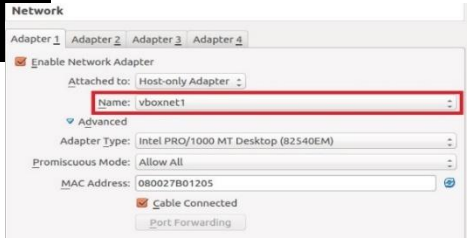
- Create and Configure Guest VM (VirtualBox)

◎ Install Guest OS (Windows10 x64)



◎ Configure host-only network





Cuckoo Installation (Guest OS)

- To make Cuckoo run properly in the virtualized Windows system, install some required software and libraries

◎ Install Python (https://www.python.org/ftp/python/2.7.13/python-2.7.13.msi)

◎ Install Python Image libray (http://www.pythonware.com/products/pil/)

◎ Turn off windows firewall and automatic updates

◎ Install the agent

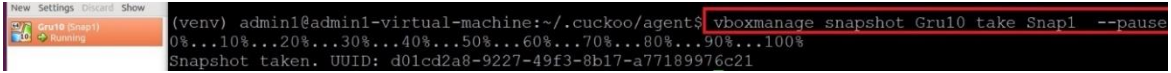
```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ pwd
/home/admin1/.cuckoo/agent
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ ls -la
total 32
drwxrwxr-x  3 admin1 admin1  4096 Aug 12 20:01 .
drwxrwxr-x 14 admin1 admin1  4096 Aug 11 16:20 ..
-rw-rw-r--  1 admin1 admin1 12307 Aug 11 09:56 agent.py
-rwxrwxr-x  1 admin1 admin1   386 Aug 11 09:56 agent.sh
drwxrwxr-x  3 admin1 admin1  4096 Aug 12 20:01 android
```

```
PS C:¥Users¥UserOk¥Downloads> dir

    ディレクトリ: C:¥Users¥UserOk¥Downloads

Mode                LastWriteTime         Length Name
----                -------------         ------
-a----        2017/08/13      1:56          12307 agent.py
-a----        2017/08/13      1:55
```

◎ Run the Agent

Cuckoo Installation (Guest OS)

◎ Saving the virtual machine



◎ Power off the machine and restore it

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ vboxmanage controlvm Gru10 poweroff
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ vboxmanage snapshot Gru10 restorecurrent
Restoring snapshot d01cd2a8-9227-49f3-8b17-a77189976c21
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

◎ Edit virtualbox.conf

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ pwd
/home/admin1/.cuckoo/conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ file virtualbox.conf
virtualbox.conf: ASCII text
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ more virtualbox.conf
[virtualbox]
# Specify which VirtualBox mode you want to run your machines on.
# Can be "gui" or "headless". Please refer to VirtualBox's official
# documentation to understand the differences.
mode = headless

# Path to the local installation of the VBoxManage utility.
path = /usr/bin/VBoxManage
# If you are running Cuckoo on Mac OS X you have to change the path as follows:
# path = /Applications/VirtualBox.app/Contents/MacOS/VBoxManage

# Default network interface.
interface = vboxnet1

# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1


[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = Gru10

# Specify the operating system platform used by current machine
# [windows/darwin/linux].
platform = windows

# Specify the IP address of the current virtual machine. Make sure that the
# IP address is valid and that the host machine is able to reach it. If not,
# the analysis will fail.
ip = 192.168.57.2
```

Cuckoo Installation (Guest OS)

◎ Edit cuckoo.conf and configure guest vm IP as needed

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ pwd
/home/admin1/.cuckoo/conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ file cuckoo.conf
cuckoo.conf: ASCII text
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ grep resultserver_ip --color cuckoo.conf  -A 1
# `resultserver ip` for all your virtual machines in machinery configuration.
ip = 192.168.57.1
```

◎ Edit reporting.conf and enable elastic search (enables Web Interface serach feature)

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ pwd
/home/admin1/.cuckoo/conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ grep elasticsearch --color reporting.conf  -A 1
[elasticsearch]
enabled = yes
```

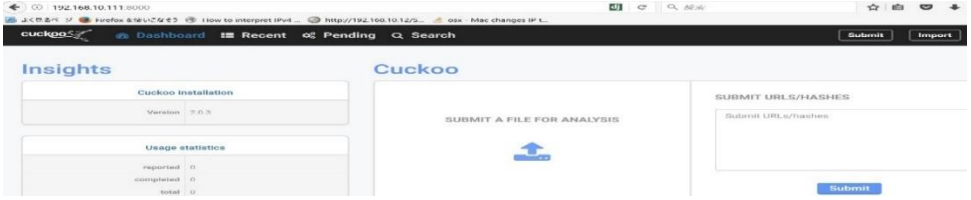
Cuckoo: Web interface

- Web interface in the form of a Django application (can use Django web interface or use an webserver such as nginx)
- Enable MongoDB

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ pwd
/home/admin1/.cuckoo/conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ ls
auxiliary.conf  cuckoo.conf  kvm.conf     physical.conf    qemu.conf       routing.conf     vmware.conf   xenserver.conf
avd.conf        esx.conf     memory.conf  processing.conf  reporting.conf  virtualbox.conf  vsphere.conf
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ grep  --color mongodb reporting.conf -A 1
[mongodb]
enabled = yes
```

- Starting the Web Interface

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/web$ cuckoo web runserver 192.168.10.111:8000
Performing system checks...

System check identified no issues (0 silenced).
August 12, 2017 - 19:37:40
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://192.168.10.111:8000/
Quit the server with CONTROL-C.
```

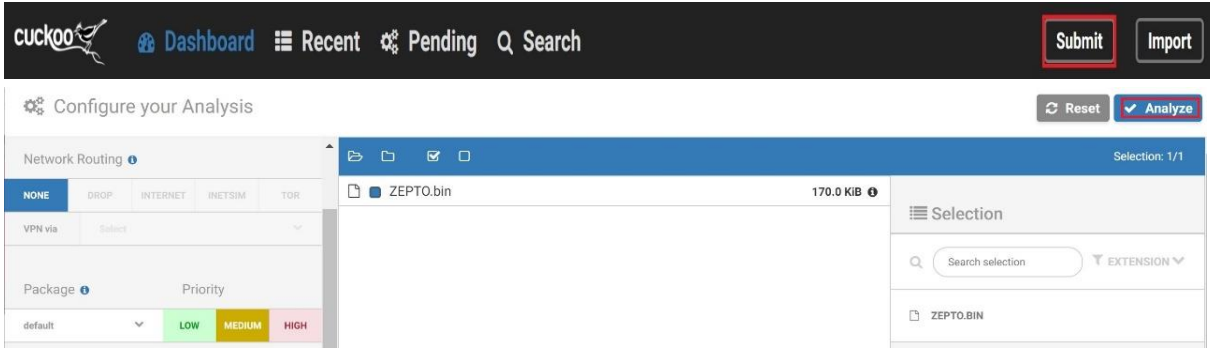


Cuckoo: Web interface and submitting files

- Run Cuckoo

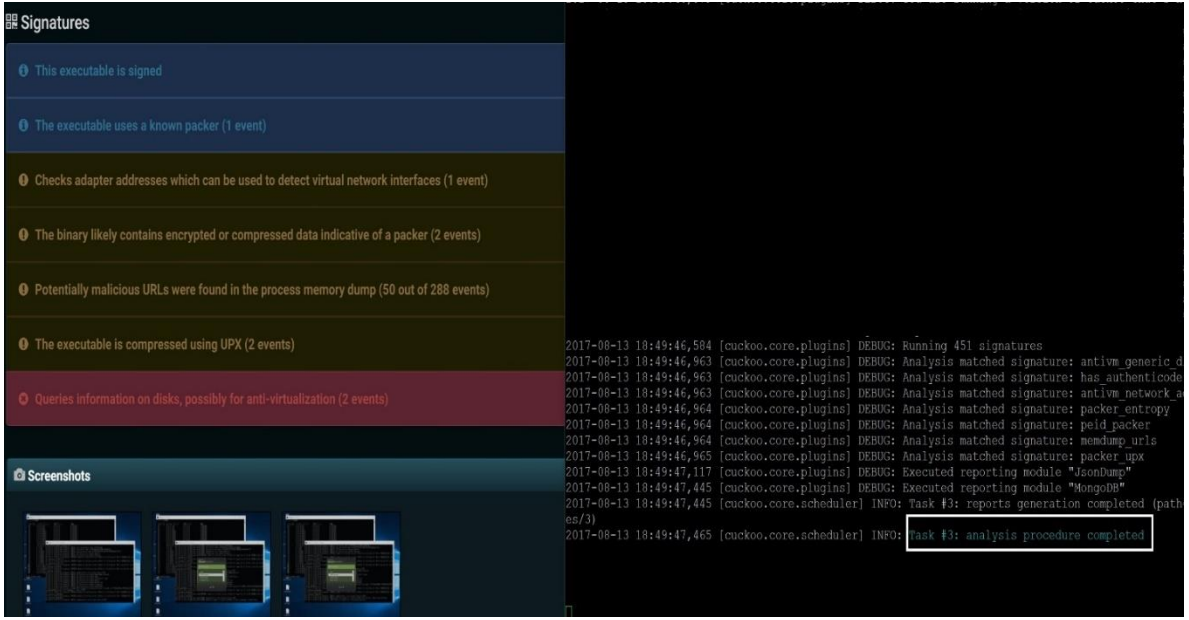
```
[cuckoo.core.resultserver] DEBUG: ResultServer running on 192.168.57.1:2042.
[cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
[cuckoo.machinery.virtualbox] DEBUG: Stopping vm Gru10
[cuckoo.machinery.virtualbox] DEBUG: Restoring virtual machine Gru10 to its current snapshot
[cuckoo.core.scheduler] INFO: Loaded 1 machine/s
[cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
(venv) admin1@admin1-virtual-machine:~/.cuckoo/conf$ cuckoo -d
```

- Submit a file from Django Web Interface (can use Django web interface or use an webserver such as nginx)



Cuckoo: Web interface and submitting files

- Analysis complete



Cuckoo: Web interface and submitting files

- Analysis log path

```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/storage/analyses/3$ pwd
/home/admin1/.cuckoo/storage/analyses/3
(venv) admin1@admin1-virtual-machine:~/.cuckoo/storage/analyses/3$ ls -la
total 76
drwxrwxr-x 8 admin1 admin1  4096 Aug 13 18:49 .
drwxrwxr-x 5 admin1 admin1  4096 Aug 13 18:49 ..
-rw-rw-r-- 1 admin1 admin1  2546 Aug 13 18:49 analysis.log
lrwxrwxrwx 1 admin1 admin1   102 Aug 13 18:47 binary -> /home/admin1/.cuckoo/storage/binaries/59720872b3d82f12a4c8aca1246a6888084186
996ef595ab4e80dd06c78c9e4
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:47 buffer
-rw-rw-r-- 1 admin1 admin1 21753 Aug 13 18:49 cuckoo.log
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:47 files
-rw-rw-r-- 1 admin1 admin1   279 Aug 13 18:49 files.json
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:47 logs
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:49 memory
-rw-rw-r-- 1 admin1 admin1   167 Aug 13 18:49 reboot.json
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:49 reports
drwxrwxr-x 2 admin1 admin1  4096 Aug 13 18:49 shots
-rw-rw-r-- 1 admin1 admin1   819 Aug 13 18:49 task.json
-rw-rw-r-- 1 admin1 admin1     0 Aug 13 18:49 tlsmaster.txt
```

References

- Cuckoo website
https://cuckoosandbox.org

- GitHub
https://github.com/cuckoosandbox/cuckoo