Install a Cuckoo Sandbox in 12 steps

[Agent.ova](https://drive.google.com/u/0/uc?id=1uGxNwvSuSIhokeuX9N61D8VtyFDoK0-2&export=download)

It is noteworthy that I completed the installation on version of Ubuntu 18.04.5 Desktop, the Cuckoo sandbox is the version of 2.0.7. If everything goes well, the following method should also support version of Ubuntu Server.

Start installation

step 1: Install system updates and update system dependencies after installing Ubuntu

$ sudo apt-get update && sudo apt-get upgrade

step 2: Install basic system dependencies by Cuckoo required (if iptables-persistent configuration GUI window pops up, keep the default selection and go on)

$ sudo apt-get install -y virtualbox vim curl net-tools htop python python-pip python-dev libffi-dev libssl-dev python-virtualenv python-setuptools python-magic python-libvirt ssdeep libjpeg-dev zlib1g-dev swig mongodb postgresql libpq-dev build-essential git libpcre3 libpcre3-dev libpcre++-dev libfuzzy-dev automake make libtool gcc tcpdump dh-autoreconf flex bison libjansson-dev libmagic-dev libyaml-dev libpython2.7-dev tcpdump apparmor-utils iptables-persistent

step 3: Update PIP and install Python dependencies

$ sudo pip install --upgrade pip

$ sudo pip install -U gdown==3.10.0 sqlalchemy==1.3.3 pefile==2019.4.18 pyrsistent==0.17.0 dpkt==1.8.7 jinja2==2.9.6 pymongo==3.0.3 bottle yara-python==3.6.3 requests==2.13.0 python-dateutil==2.4.2 chardet==2.3.0 setuptools psycopg2 pycrypto pydeep distorm3 cuckoo==2.0.7 weasyprint==0.36 m2crypto openpyxl ujson pycrypto pytz pyOpenSSL

step 4: Uninstall Werkzeug and reinstall (Werkzeug has a version update which leads to incompatibility with Cuckoo 2.0.7)

$ sudo pip uninstall werkzeug && sudo pip install werkzeug==0.16.1

step 5: Install pySSDeep, yara and volatility

$ git clone https://github.com/bunzen/pySSDeep.git && cd pySSDeep && sudo python setup.py build && sudo python setup.py install

$ wget https://github.com/VirusTotal/yara/archive/v3.7.1.tar.gz && tar -xzvf v3.7.1.tar.gz && cd yara-3.7.1 && sudo ./bootstrap.sh && sudo ./configure --with-crypto --enable-cuckoo --enable-magic && sudo make && sudo make install

$ git clone https://github.com/volatilityfoundation/volatility.git && cd volatility && sudo python setup.py build && sudo python setup.py install

step 6: Configure tcpdump and system DNS

$ sudo aa-disable /usr/sbin/tcpdump && sudo setcap cap\_net\_raw,cap\_net\_admin=eip /usr/sbin/tcpdump

$ sudo sed -i "s/127.0.0.53/8.8.8.8/g" /etc/resolv.conf

step 7: Start MongoDB service and initialize Cuckoo, pull community signatures

$ sudo service mongodb start && cuckoo && cuckoo community

step 8: Use VboxManage to create a hostonly ethernet adapter vboxnet0, and modify the default storage directory and permission for virtual machine files

$ vboxmanage hostonlyif create && vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask 255.255.255.0

$ sudo mkdir /data && sudo mkdir /data/VirtualBoxVms && sudo chmod 777 /data/VirtualBoxVms

$ vboxmanage setproperty machinefolder /data/VirtualBoxVms

step 9: Import Agent.ova, boot up to take a snapshot, and add to Cuckoo

$ vboxmanage import ~/Downloads/Agent.ova && vboxmanage modifyvm "Agent" --name "cuckoo1" && vboxmanage startvm "cuckoo1" && sleep 1m

$ vboxmanage snapshot "cuckoo1" take "snap1" && vboxmanage controlvm "cuckoo1" poweroff

$ cuckoo machine --delete cuckoo1 && cuckoo machine --add cuckoo1 192.168.56.101 --platform windows --snapshot snap1

step 10: Configure iptables to enable IP forwarding

$ sudo iptables -A FORWARD -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT && sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT && sudo iptables -A POSTROUTING -t nat -j MASQUERADE

$ sudo vim /etc/sysctl.conf

#net.ipv4.ip\_forward = 1 > net.ipv4.ip\_forward = 1

$ sudo sysctl -p /etc/sysctl.conf && sudo netfilter-persistent save

step 11: Modify the Cuckoo configuration file, open MongoDB and VirusTotal

$ vim ~/.cuckoo/conf/reporting.conf

# Change mongodb status from off to on

[mongodb]

enabled = yes

$ vim ~/.cuckoo/conf/processing.conf

# Change virustotal status from off to on

[virustotal]

enabled = yes

step 12: Run Cuckoo

$ cuckoo

$ cuckoo web -H 0.0.0.0 -p 8000

You just need to prepare a clean Ubuntu and run following command:

bash <(curl -sS -L https://raw.githubusercontent.com/S4kur4/AutoDeployCuckoo/master/install.sh)

The code is here: [AutoDeployCuckoo](https://github.com/S4kur4/AutoDeployCuckoo)