Cuckoo sandbox 安裝流程

環境:

- Host: Ubuntu 16.04.7 LTS
- Guest: windows 7

事前準備

更新

```
sudo apt-get update
```

安裝相關套件

```
sudo apt-get install python-sqlalchemy python-bson
sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
sudo apt-get install python-virtualenv python-setuptools
sudo apt-get install libjpeg-dev zlib1g-dev swig
sudo apt-get install libtool automake libmagic-dev
sudo apt-get install mongodb
sudo apt-get install postgresql libpq-dev
```

安裝 virtual box

```
sudo apt-get install virtualbox
```

安裝 Yara

```
wget https://github.com/VirusTotal/yara/archive/v3.4.0.tar.gz
tar xvfz v3.4.0.tar.gz
cd yara-3.4.0/
./bootstrap.sh
./configure --enable-cuckoo --enable-magic
make
sudo make install
```

安裝 tcpdump

```
sudo apt-get install tcpdump apparmor-utils
sudo aa-disable /usr/sbin/tcpdump
```

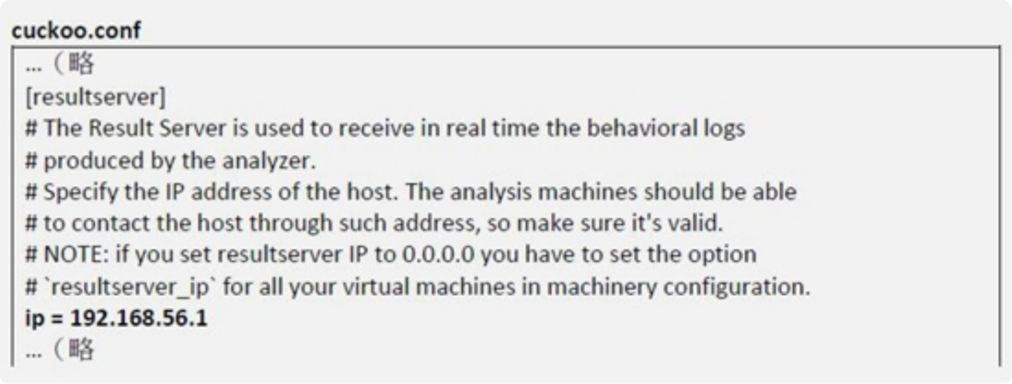
安裝 cuckoo

```
sudo pip install -U pip==20.3.4 setuptools==44.1.1
sudo pip install -U cuckoo
```

設定 cuckoo

config 設定

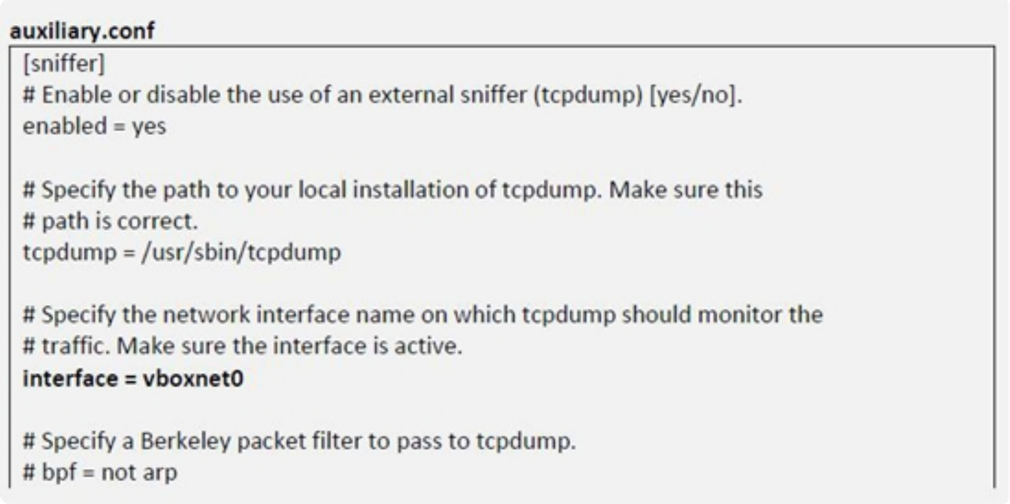
- 需修改 /home/ubuntu/.cuckoo/conf 中，cuckoo.conf、auxiliary.conf、virtualbox.conf
- 此處所說的resultserver即為Cuckoo host，此處的IP用於讓Analysis Guests傳輸資訊，因此須設定Virtual network網段的IP。



cuckoo.conf

```
...（略
[resultserver]
# The Result Server is used to receive in real time the behavioral logs
# produced by the analyzer.
# Specify the IP address of the host. The analysis machines should be able
# to contact the host through such address, so make sure it's valid.
# NOTE: if you set resultserver IP to 0.0.0.0 you have to set the option
# `resultserver_ip` for all your virtual machines in machinery configuration.
ip = 192.168.56.1
...（略
```

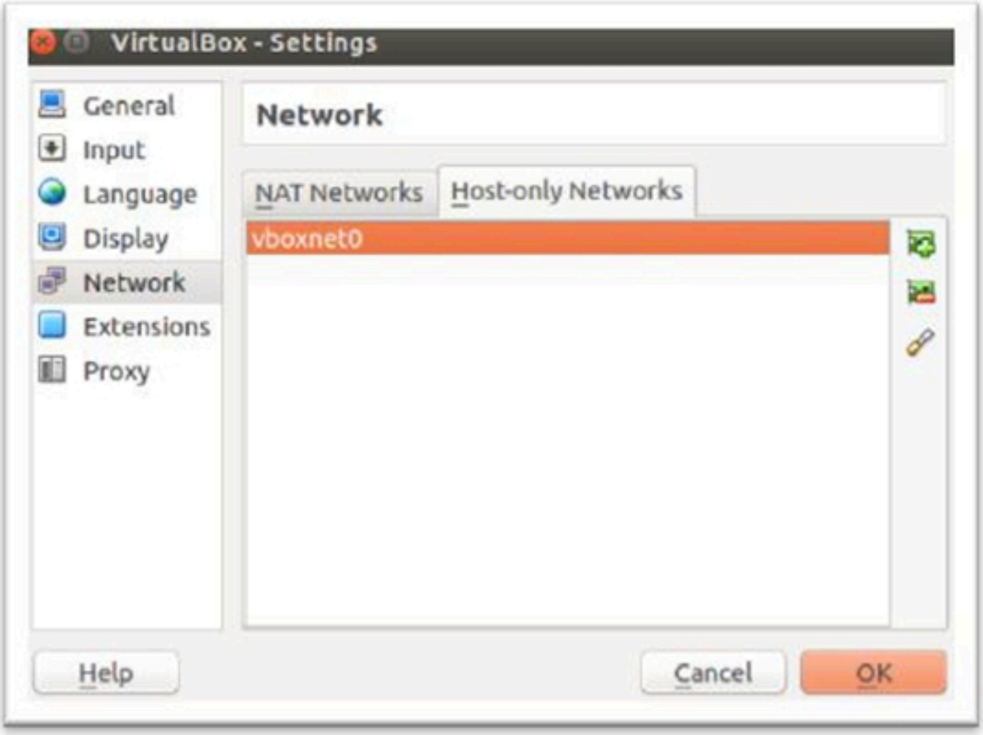
- vboxnet0 為 VirtualBox的虛擬網路介面，預設是沒有此介面的，需要手動新增。



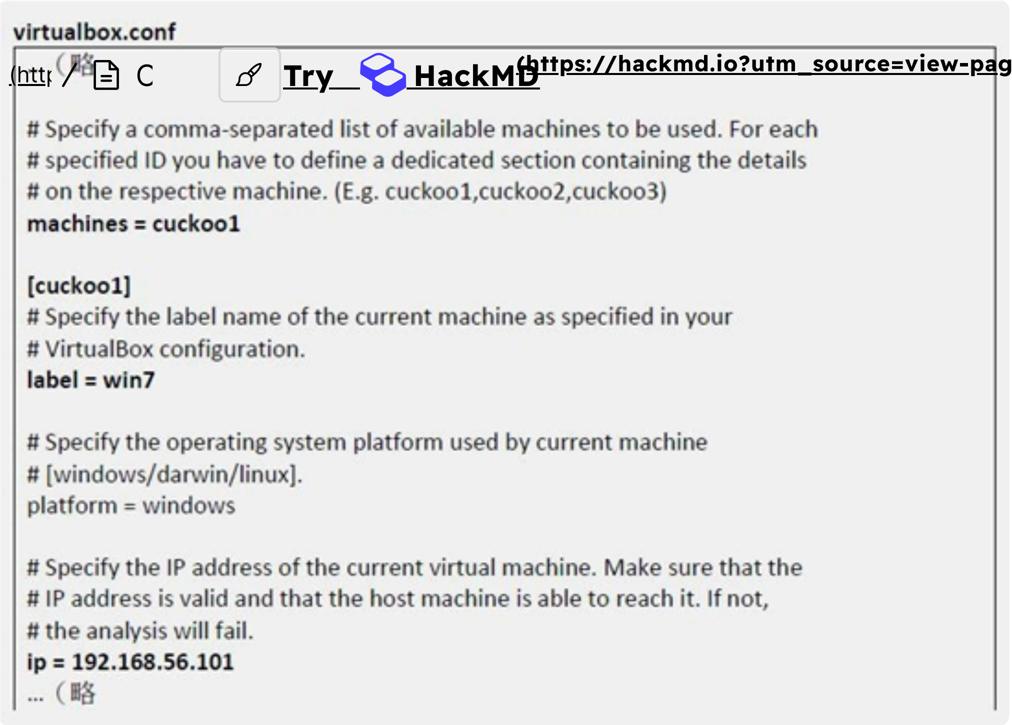
auxiliary.conf

```
[sniffer]
# Enable or disable the use of an external sniffer (tcpdump) [yes/no].
enabled = yes

# Specify the path to your local installation of tcpdump. Make sure this
# path is correct.
tcpdump = /usr/sbin/tcpdump

# Specify the network interface name on which tcpdump should monitor the
# traffic. Make sure the interface is active.
interface = vboxnet0

# Specify a Berkeley packet filter to pass to tcpdump.
# bpf = not arp
```

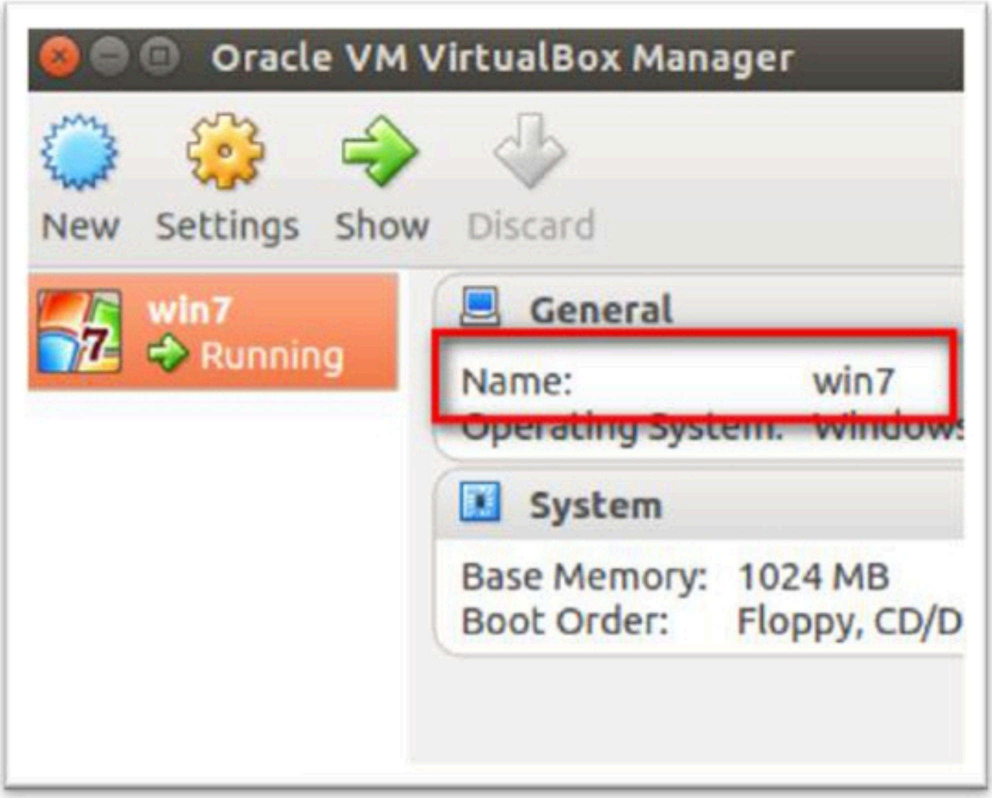
- 需新增 Host-only Networks，IPv4 位址設為 192.168.56.1，IPv4 網路遮罩設為 255.255.255.0



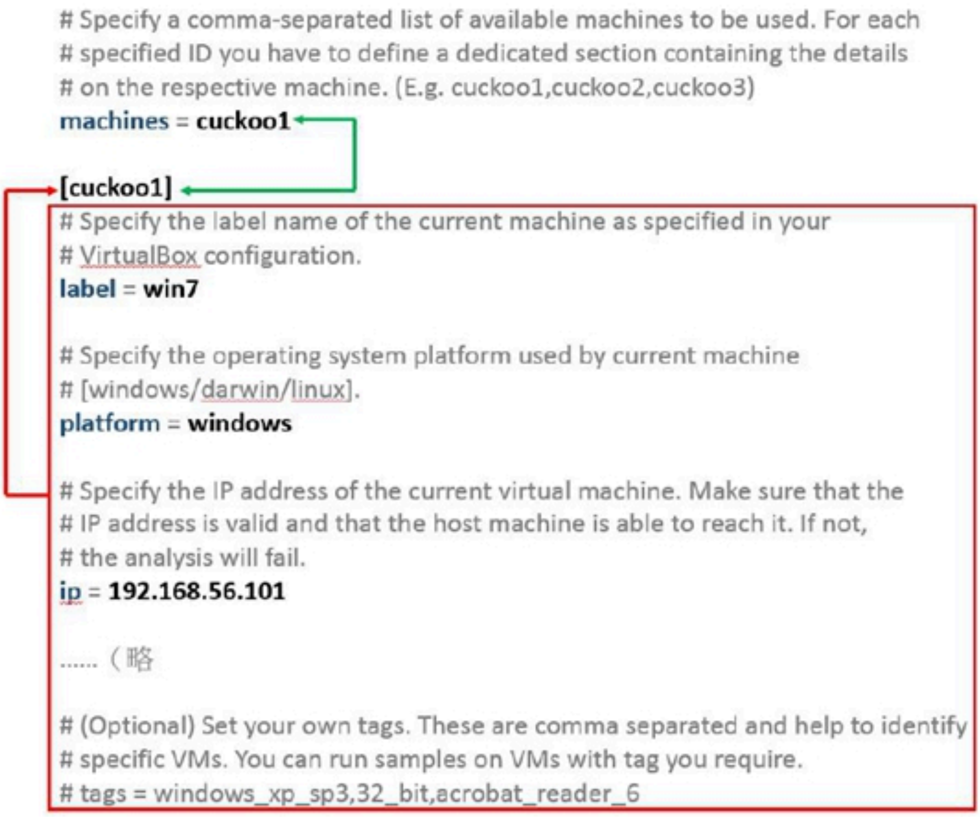
- 在此設定檔中，有幾個參數需要特別做說明，cuckoo允許載入多個Analysis guest，透過參數『machines』可以載入多個Guest的設定（如圖示），以此設定檔為例 [cuckoo1] 即為一個Guest的設定（如圖示），cuckoo1為此設定的名稱（須與machines設定的名稱相同），而『label』則是此虛擬機的名稱（如圖示），IP則是Guest的IP address。



```
virtualbox.conf
（略

# 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 = win7

# 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 = 192.168.56.101
... （略
```



Name: win7
Operating System: Windows
Base Memory: 1024 MB
Boot Order: Floppy, CD/D

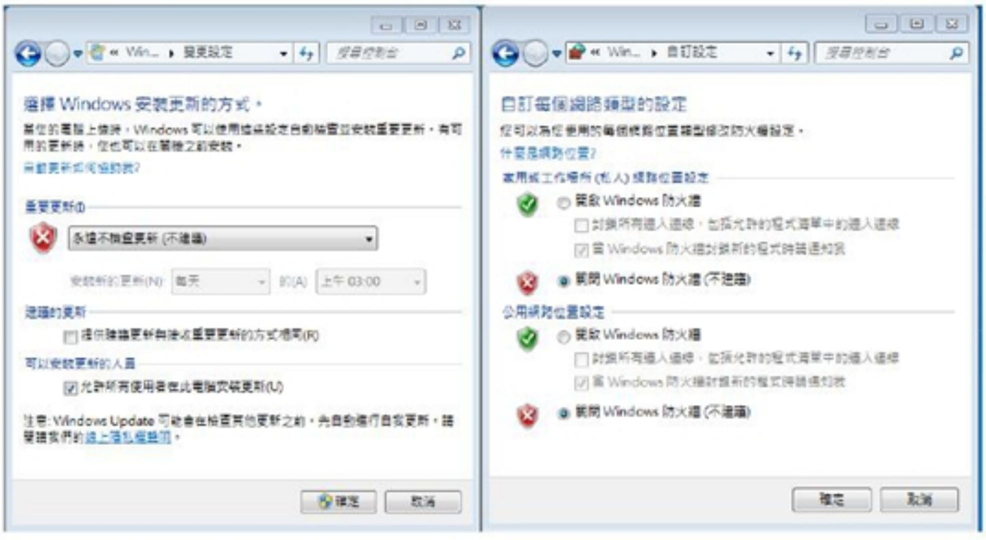


```
# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1

[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = win7

# 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 = 192.168.56.101

......（略

# (Optional) Set your own tags. These are comma separated and help to identify
# specific VMs. You can run samples on VMs with tag you require.
# tags = windows_xp_sp3,32_bit,acrobat_reader_6
```

虛擬機設定

關閉自動更新、防火牆

- 控制台→系統及安全性→Windows Update下的開啟或關閉自動更新
- 控制台→系統及安全性→Windows 防火牆→開啟或關閉 Windows 防火牆→關閉 Windows 防火牆



選擇 Windows 安裝更新的方式。

當您的電腦上線時，Windows 可以使用這些設定自動檢查並安裝重要更新。有可用的更新時，您也可以在關機之前安裝。

自動更新如何協助我?

重要更新(I)

永遠不檢查更新 (不建議)

安裝新的更新(N): 每天 於(A) 上午 03:00

建議的更新

☐ 提供建議更新與接收重要更新的方式相同(R)

可以安裝更新的人員

☑ 允許所有使用者在此電腦安裝更新(U)

注意: Windows Update 可能會在檢查其他更新之前，先自動進行自我更新。請閱讀我們的線上隱私權聲明。

確定 取消

自訂每個網路類型的設定

您可以為您使用的每個網路位置類型修改防火牆設定。

什麼是網路位置?

家用或工作場所 (私人) 網路位置設定

○ 開啟 Windows 防火牆

☐ 封鎖所有連入連線，包括允許的程式清單中的連入連線

☑ 當 Windows 防火牆封鎖新的程式時通知我

● 關閉 Windows 防火牆 (不建議)

公用網路位置設定

○ 開啟 Windows 防火牆

☐ 封鎖所有連入連線，包括允許的程式清單中的連入連線

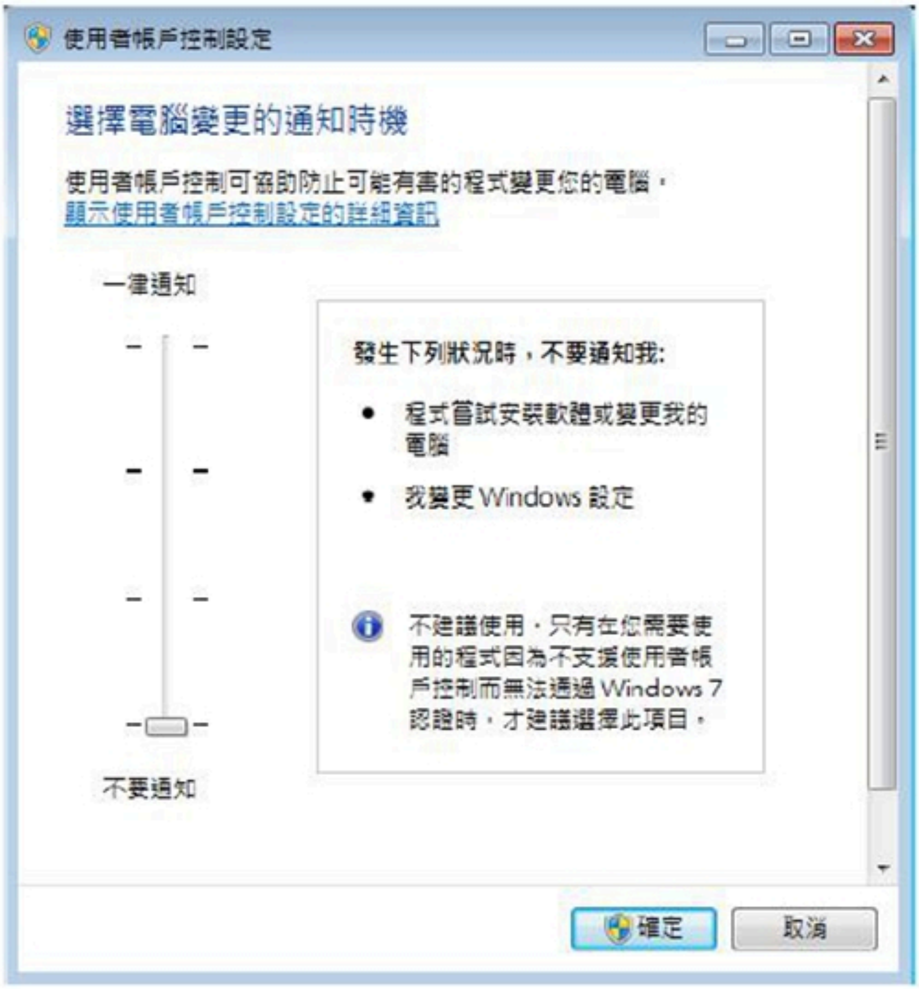
☑ 當 Windows 防火牆封鎖新的程式時通知我

● 關閉 Windows 防火牆 (不建議)

確定 取消

關閉 UAC

- 控制台→使用者帳戶和家庭安全→使用者帳戶→變更使用者帳戶控制設定



使用者帳戶控制設定

選擇電腦變更的通知時機

使用者帳戶控制可協助防止可能有害的程式變更您的電腦。

顯示使用者帳戶控制設定的詳細資訊

一律通知

不要通知

發生下列狀況時，不要通知我:

- 程式嘗試安裝軟體或變更我的電腦
- 我變更 Windows 設定

不建議使用。只有在您需要使用的程式因為不支援使用者帳戶控制而無法通過 Windows 7 認證時，才建議選擇此項目。

確定 取消

設置靜態 IP

- 將虛擬機設置靜態 IP ，IP 需與 virtualbox.conf 中 ip 一致

在虛擬機中安裝 python 2.7

- 須注意 windows 是 64bit 或是 32bit

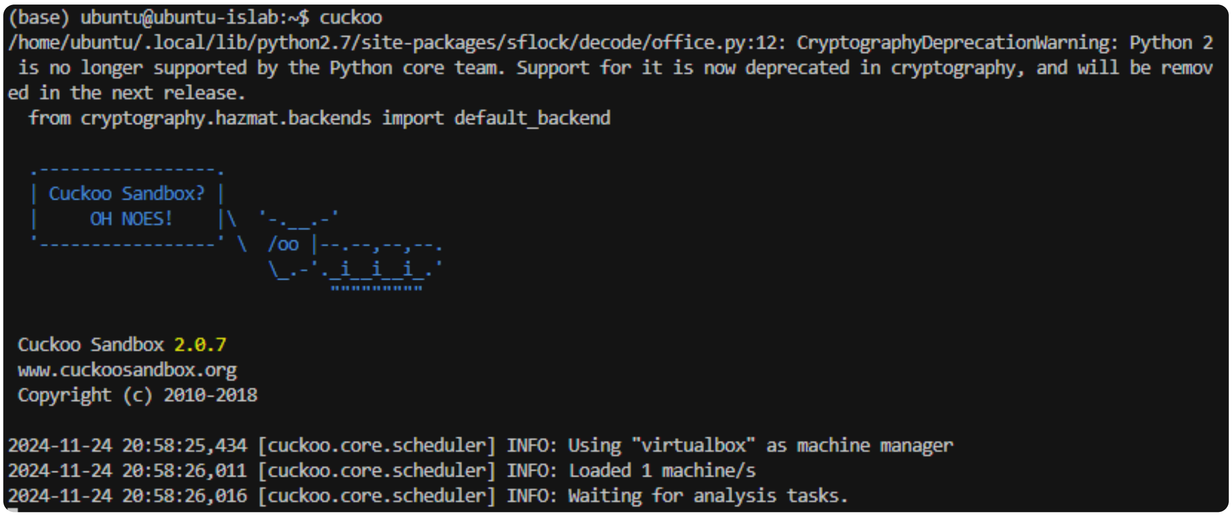
Agent 設定

- agent.py (http://agent.py) 位置在 /home/ubuntu/.cuckoo/agent 中，將 agent.py (http://agent.py) 透過 vm 共用資料夾放進虛擬機中
- 執行 agent 後，將此狀態做 snapshot
- 在 virtualbox.conf 中將 snapshot 改為此 snapshot，如：

```
# (Optional) Specify the snapshot name to use. If you do not specify a snapshot
# name, the VirtualBox MachineManager will use the current snapshot.
# Example (Snapshot1 is the snapshot name):
snapshot = Snapshot 1
```

執行 cuckoo

- 在 terminal 中執行 cuckoo，應出現



```
(base) ubuntu@ubuntu-islab:~$ cuckoo
/home/ubuntu/.local/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 remov
ed in the next release.
  from cryptography.hazmat.backends import default_backend

  .-----------------.
  | Cuckoo Sandbox? |
  |     OH NOES!    |\  '-.__.-'
  '-----------------' \  /oo |--.--,--,--.
                         \_.-'._i__i__i_.'
                               """""""""

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

2024-11-24 20:58:25,434 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2024-11-24 20:58:26,011 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2024-11-24 20:58:26,016 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
```

參考資料

來源:

- https://cuckoo.readthedocs.io/en/latest/installation/ (https://cuckoo.readthedocs.io/en/latest/installation/)
- https://www.syscom.com.tw/ePaper_New_Content.aspx?id=446&EPID=208&TableName=sgEPArticle (https://www.syscom.com.tw/ePaper_New_Content.aspx?id=446&EPID=208&TableName=sgEPArticle)
- https://jameshclai.blogspot.com/2017/03/how-to-install-cuckoo-sandbox-step1.html (https://jameshclai.blogspot.com/2017/03/how-to-install-cuckoo-sandbox-step1.html)
- https://www.cnblogs.com/BenjaminNL/p/11139517.html (https://www.cnblogs.com/BenjaminNL/p/11139517.html)
- https://blog.csdn.net/2401_83974590/article/details/137646626 (https://blog.csdn.net/2401_83974590/article/details/137646626)