Cuckoo installation on ubuntu with VirtualBox (win7 x64)

Cuckoo sandbox簡介

Cuckoo Sandbox起於2010年Honeynet其中一個專案，直到2011年realse版才正式釋出，現在的版本為1.1，是一個基於虛擬化環境所建立的惡意程式分析系統，能自動執行並且分析檔案，同時紀錄以下資訊：

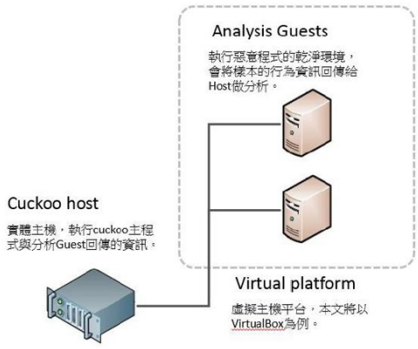
- 追蹤程式Process
- 程式對於檔案的異動
- Memory dump
- 程式的網路行為
- 程式運作過程中，Windows桌面截圖

環境介紹

Cuckoo系統主要分成三個部份：Cuckoo host、Analysis Guests、Virtual platform，Virtual platform建置於cuckoo host上，提供Analysis guest虛擬環境紀錄惡意程式的行為，而後在cuckoo host做分析，cuckoo系統管理與執行也是在cuckoo host做操作，以下是我們使用的os與軟體資訊：

環境資訊

平台	OS/software
Cuckoo host	Ubuntu 16.04
Analysis Guest	Windows 7 Enterprise (x64)
Virtual platform	VirtualBox



Preparing the Host:

在安裝Cuckoo之前，我們有一些套件及工具需要安裝

首先，到Cuckoo的official doc:
https://cuckoo.sh/docs/installation/host/requirements.html

網頁中包含需要安裝的套件(有些為optional)有哪些，打開terminal後輸入:

```
$ 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
```

💡 補充: 因為Cuckoo目前對python3僅部分相容，官網也建議大家使用python2.7，這也是我們當初選用Ubuntu16.04的原因之一，因為Ubuntu16.04的OS已有包含python2.7

接著，如果選擇使用Django框架作為網頁介面的話，便需要安裝MongoDB

```
$ sudo apt-get install mongodb
```

在資料庫方面，官方則建議用PostgreSQL

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

Host端到這邊算完成一部份了，我們接下來在Host上安裝Virtual platform，官網的範例是用VirtualBox，可以直接至其官網下載最新版本

為了記錄惡意程式所做的網路活動 (Network sniffer)，我們需要安裝tcptump在Ubuntu上

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

Guacd is an optional service that provides the translation layer for RDP, VNC, and SSH for the remote control functionality in the Cuckoo web interface. (如何合適的翻譯這段?)

```
$ sudo apt install libguac-client-rdp0 libguac-client-vnc0 libguac-client-ssh0 guacd
```

接著要設定路徑，在Cuckoo資料夾裡面(忘了幾層)有個叫'conf'的資料夾，我們至少要設定cuckoo.conf 與<machinery>.conf才能運作Cuckoo，而且他們是唯讀的，所以必須更改成root權限

> Cuckoo relies on a couple of main **conf**iguration files:
> - cuckoo.**conf**: for **conf**iguring general behavior and analysis options.
> - auxiliary.**conf**: for enabling and **conf**iguring auxiliary modules.
> - <machinery>.**conf**: for defining the options for your virtualization software (the file has the same name of the machinery module you choose in cuckoo.**conf**).
> - memory.**conf**: Volatility **conf**iguration.
> - processing.**conf**: for enabling and **conf**iguring processing modules.
> - reporting.**conf**: for enabling or disabling report formats.
> To get Cuckoo working you should at the very least edit cuckoo.**conf** and <machinery>.**conf**.

安裝Cuckoo

一切套件安裝好後，終於可以安裝Cuckoo啦~~

```
$ virtualenv venv
$ . venv/bin/activate
```

```
(venv)$ pip install -U pip setuptools
(venv)$ pip install -U cuckoo
```

到這邊為止Host和Virtual platform 就安裝完成了

Preparing the Guest:

- 官方推薦用Windows7(X64)或Windows XP，我們選擇前者
- 安裝python2.7

下載 python2.7，執行並記下該安裝位置

- 更改環境變數

路徑：開啟檔案總管>右鍵點選本機>點擊"內容">點擊左側"進階系統設定">點擊下方"環境變數">至下方系統變數尋找"Path"並點擊"編輯">將路徑更改為當初安裝python之位置

- 安裝pip

下載 get-pip.py (右鍵另存新檔)>並透過command line 執行安裝

```
$ python get-pip.py
```

- 安裝Pillow，用於在虛擬機器中截圖

```
$ pip install pillow
```

- 在guest端下載agent.py()，執行後會啟動一個API server，用來溝通host與guest，之後每次欲啟動Cuckoo時皆須打開VM執行該檔案

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/c23b814d-3fb5-4d01-92ee-22e18f2b1247/agent.py

- 設定虛擬機器網路

由於目前cuckoo不支援DHCP，Guest必須使用固定IP，使用DHCP可能會使得Host無法跟agent連線，導致cuckoo無法正常運作，而Virtual network設定為Host-Only模式，Host方面需要做Forward設定

於Virtualbox介面上方工具列中點擊"File">點擊"Host Network Manager">點擊"新增"按鈕，將會增加一個名為"Vboxnet0"的host-only network>至該VM的網路設定中啟用第二介面卡，並設定為Host-only模式

到這邊為止，Guest方面已經設定完成

安裝時的其他問題

- Ulimit maximum (4096) 更改限制

使用Cuckoo Sandbox進行分析時，可能會遇到系統預設分析資料數量上限的問題，系統預設通常為1024，此時需要至/etc/security/limits.conf文件中修改數量限制，數量部分只要確保數量夠大即可，"*"則是代表任何使用者都適用該限制。

```
* soft nofile 10000
* hard nofile 10000
```

- .cuckoo中的virtual.conf修改

由於該檔案路經位於隱藏檔(檔名前含有".")，需利用指令於純文字介面中修改。

- 啟動方式

先開啟VM，並且打開agent.py，以便隨時開始進行分析，

之後進入安裝時的環境，便可啟動cuckoo以及cuckoo web

```
$ . venv/bin/activate
$ cuckoo
$ cuckoo web
```

Reference

1. 郭毅志, “惡意程式分析沙箱 – cuckoo Sandbox,” 電腦科技電子報, vol. 208, Feb 2015. [online]. Available: https://bit.ly/2Mwb86f. [Accessed Octorber 7, 2019].