TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

ĐẠI HỌC QUỐC GIA TP.HCM

--------------------------------



**KỸ THUẬT PHÂN TÍCH MÃ ĐỘC**

**TÌM HIỂU VÀ TRIỂN KHAI HỆ THỐNG SANDBOX**

SV thực hiện:

MSSV 1: 14520677 – VŨ TẤN PHONG

MSSV 2: 14520590 – VÕ MINH NGỌC

MSSV 1: 14520757 – NGUYỄN KIM SANG

MSSV 2: 14520387 – TRẦN THANH HUY

Lớp: NT137.I21.ANTT

GV: **NGUYỄN TẤN CẦM**

# HẬN XÉT CỦA GVHD

……………………………………………………………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

Chữ ký GVHD:

…………………………………..

**MỤC LỤC**

# Lời mở đầu

Trước xu thế các cuộc tấn công mạng đang gia tăng về cả số lượng, chất lượng cũng như độ phức tạp, các giải pháp phòng ngừa và ngăn chặn là rất cần thiết. Hàng loạt các giải pháp được đưa ra như: Firewall, IDS/IPS, WAF, Honeypot… Một trong những giải pháp đó là sử dụng cơ chế Sandbox. Từ ý tưởng ấy và những gợi ý từ giáo viên hướng dẫn Ths Nguyễn Duy, nhóm đã lên ý tưởng sẽ xây dựng một hệ thống phân tích tự động các tệp tin được tải về sử dụng cơ chế Sandbox. Hệ thống Sandbox này sẽ được mô phỏng trên cloud giống như một stand-alone server cung cấp cho nhiều người dùng. Quá trình xây dựng mô hình và hiện thực hóa ý tưởng trên của nhóm gặp rất nhiều khó khăn khi các tài liệu hạn chế cũng như sự không tương thích giữa phần mềm và phần cứng. Tuy nhiên với sự chăm chỉ và không nản chí dù trải qua rất nhiều thất bại nhóm đã hoàn thành ý tưởng một cách tốt đẹp.

Cám ơn.

PHẦN 1: TỔNG QUAN VỀ CUCKOO SANDBOX

I. Giới thiệu Cuckoo Sandbox:

1.1. Khái niệm Sandbox:



Trong bảo mật máy tính, Sandbox là một cơ chế cách ly các chương trình đang chạy. Hệ thống này được sử dụng để thực thi các chương trình hoặc mã lệnh chưa được kiểm định hoặc từ những nguồn ko tin cậy, có thể đến từ các bên thứ 3, người dùng hoặc các web không an toàn mà không ảnh hưởng tới máy chủ thể và hệ điều hành.

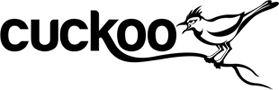
Một Sandbox thường quản lý một cách chặt chẽ các tài nguyên được cấp cho các chương trình guest chạy. Ví dụ như “scratch space” trên đĩa cứng hoặc ram. Truy cập mạng, khả năng điều tra máy chủ thể hoặc đọc từ các thiết bị đầu vào thường bị hạn chế hoặc cấm tuyệt đối.

Tóm lại Sandbox cung cấp một môi trường được kiểm soát chặt chẽ, có thể được xem là một ví dụ điển hình của ảo hóa. Môi trường Sandbox thường được sử dụng cho mục đích kiểm tra các chương trình chưa được kiểm định mà trong đó có thể chứa virus hoặc mã độc mà không ảnh hưởng đến máy chủ thể.

Sandboxie là các phần mềm dựa trên cơ chế sandbox, cung cấp một môi trường để cách ly các phần mềm chạy bên trong nó với bên ngoài.

Từ cơ chế Sandbox, các công cụ dựa trên sandbox ra đời với mục đích tự động hóa các công việc phức tạp của việc phân tích mã độc. Các công cụ như: Cuckoo Sandbox, Limon Sandbox, Fireeye, VirusTotal, Anubis, Malwr, …

1.2. Cuckoo Sandbox là gì:

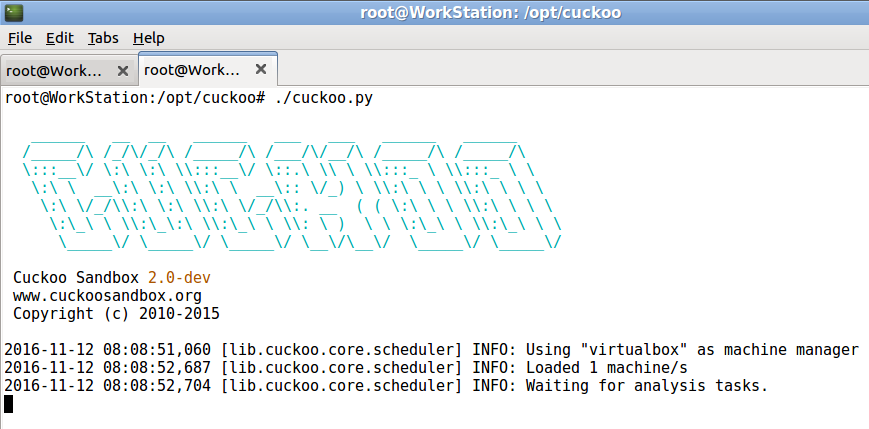


Cuckoo Sandbox là một hệ thống tự động hóa việc phân tích phần mềm độc hại. Nói cách khác, bạn có thể ném cho nó một gói tin đáng ngờ nào đó và chỉ vài giây sau Cuckoo Sandbox sẽ cung cấp cho bạn một số kết quả chi tiết phác hoạ những gì tập tin như vậy đã làm khi thực hiện trong một môi trường cô lập.

Cuckoo Sandbox là một phần mềm miễn phí tự động phân tích các tập tin độc hại trên Windows, OS X, Linux và Android.

Đây là một project bắt đầu vào năm 2010 là một phần của The Honeynet Project thuộc Google Summer of Code 2010. Được thiết kế và phát triển bởi Claudio “nex” Guarnieri, người hiện tại vẫn là project leader và core developer của dự án.

Bản beta đầu tiên được phát hành vào 05/02/2011. Vào cuối tháng 1 năm 2012, trang web Malwr.com được mở, một phiên bản Cuckoo Sandbox miễn phí và chạy trên nền công cộng với một giao diện đầy đủ thông qua đó người dùng có thể gửi các tệp được phân tích và thu được kết quả. Tháng 09/2014 Cuckoo Sandbox 1.0 được phát hành và gần nhất 21/02/2016 phiên bản 2.0 được giới thiệu.



Hình 1: Cuckoo Sandbox 2.0

Cộng đồng sử dụng: <https://community.cuckoosandbox.org/>. Thay vào đó Cuckoo Sandbox có một IRC server hỗ trợ real-time, nếu bạn có bất cứ khó khăn nào hãy liên hệ thông qua IRC server này:

Server: irc.freenode.net

Channel: #cuckoosandbox

Một vài lệnh cơ bản:

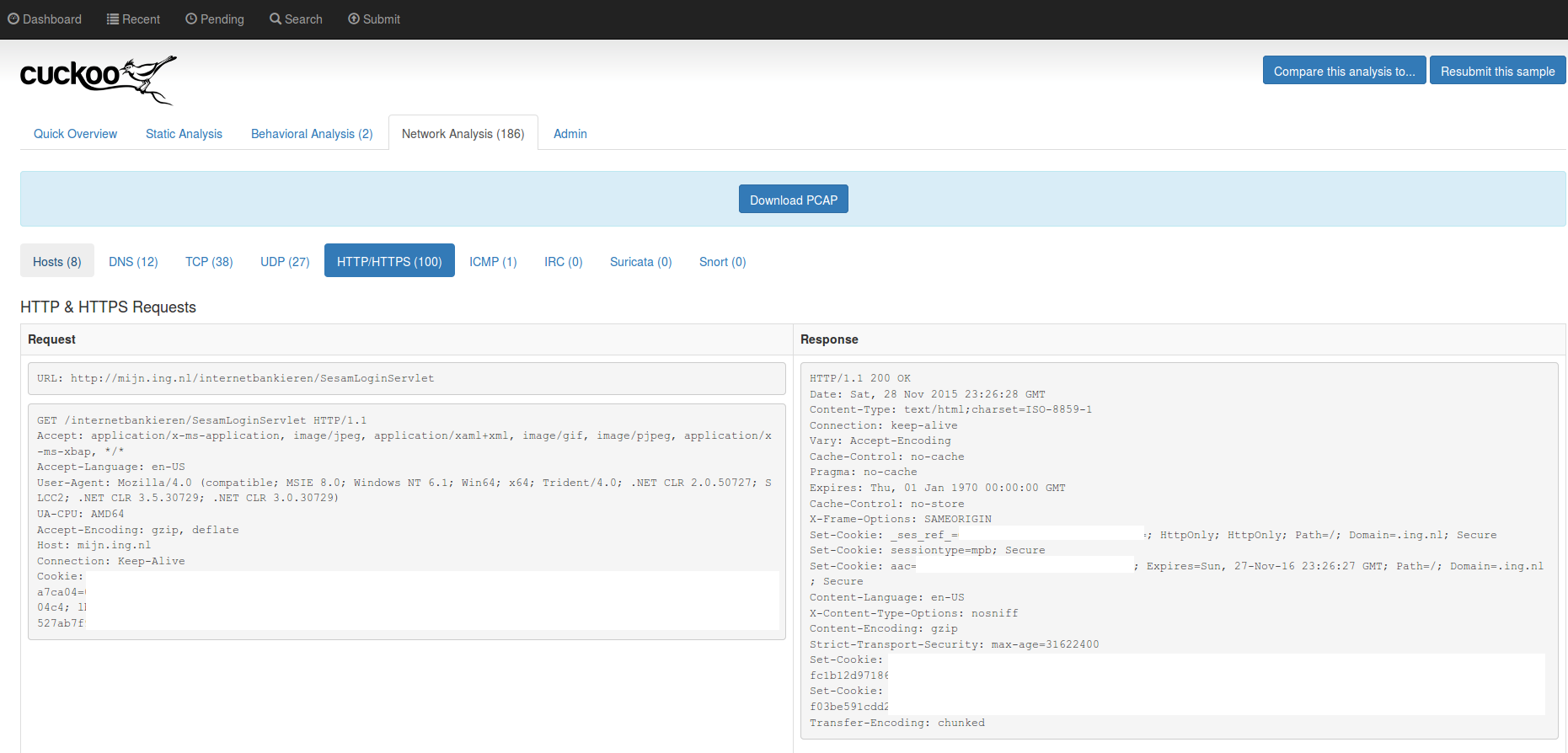
* /join #channel để tham gia channel
* /part #channel để rời channel
* /nick Nickname để thay đổi nickname
* /query Someone để giao tiếp riêng tư với một người
* /who để xem danh sách các người dùng đang hoạt động trên channel
* /help để xem toàn bộ các câu lệnh

1.3. Tính năng của Cuckoo Sandbox:

Cuckoo Sandbox được viết theo kiến trúc modular, 100% open source và nhiều tiềm năng trong việc ứng dụng.

Mặc định Cuckoo Sandbox có thể:

* Phân tích các tệp độc hại khác nhau (file thực thi, các file văn bản bị khai thác hoặc java applet) cũng như các website độc hại trên Windows, Linux, OSX và Android.
* Theo dõi các lời gọi API được tạo ra bởi hành động của file đang phân tích.
* Dump và phân tích lưu lượng mạng, thậm chí là khi đã encrypted.
* Thực hiện phân tích nâng cao memory của hệ thống máy ảo đã bị lây nhiễm với sự kế thừa từ framework volatility.



Hình 2: HTTP & HTTP Requests

1.4.Tính tùy biến của Cuckoo Sandbox:

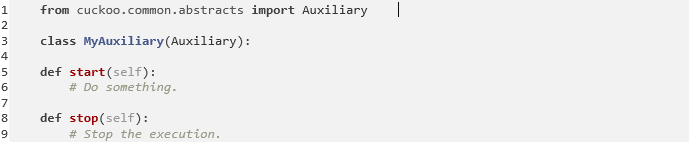
Nhờ vào thiết kế modular (module mở rộng) bạn có thể tùy chỉnh cả quá trình xử lý và giai đoạn báo cáo. Cuckoo cung cấp cho bạn tất cả các yêu cầu để dễ dàng tích hợp các sandbox vào các khuôn khổ hiện có của bạn và với dữ liệu bạn muốn, theo cách bạn muốn, với định dạng mà bạn muốn.

Các module của Cuckoo Sandbox:

1.4.1.Auxiliry modules:

Auxiliry module (module mở rộng) định nghĩa các thủ tục cần được thực thi song song với từng quá trình phân tích. Tất cả các module mở rộng nên được đặt trong thư mục cuckoo/cukoo/auxiliary.

Cấu trúc xương sống của một module mở rộng thường có dạng sau:



Hàm start() sẽ được thực thi trước khi khởi động máy ảo phân tích. Trong khi hàm end() sẽ được thực thi vào cuối quá trình phân tích, trước khi gửi sang các thủ tục của processing module và reporting module.

Ví dụ, một mô đun phụ trợ được cung cấp theo mặc định ở Cucuco được gọi là sniffer.py và thực hiện tcpdump để dump lưu lượng mạng được tạo ra.

Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/auxiliary/>

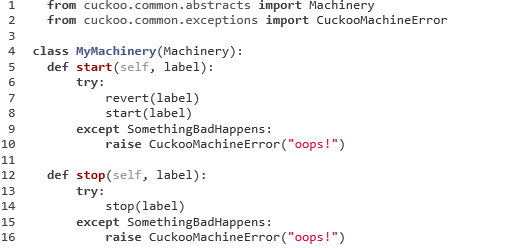
1.4.2. Machinery Modules:

Machinery Modules định nghĩa cách Cuckoo tương tác với phần mềm ảo hóa của bạn (hoặc tiềm tăng hơn là thậm chí với các giải pháp physical disk imaging).

Từ bản 0.4 do Cuckoo Sandbox không bắt buộc một nhà cung cấp ảo hóa cụ thể nào nên bạn hoàn toàn có thể sử dụng giải pháp ưa thích của mình. Trong trường hợp giải pháp ấy không được hỗ trợ mặc định bạn có thể viết module python tùy chỉnh để xác định làm thế nào để Cuckoo sử dụng nó.

Tất cả module machinery cần được đặt trong đường dẫn cuckoo/cukoo/machinery.

Một module machinery cơ bản có dạng sau:



• MyMachinery: tên class kế thừa từ Machinery.

• Start() và stop(): các hàm định nghĩa.

• CuckooMachineError: thông báo lỗi.

Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/machinery/>

1.4.3. Processing Modules:

Đây là các tập lệnh Python cho phép định nghĩa những cách tùy chọn để phân tích kết quả thô được trả về bởi sandbox và thêm một số thông tin vào “một vùng chứa toàn cục” (**global container**) vốn sẽ được dùng bởi các module signature và reporting.

Sau khi quá trình phân tích kết thúc, Cuckoo sẽ gọi tất cả các processing module có trong đường dẫn cukoo/processing/ , kết quả trả về của các module processing sẽ được lưu trong một cấu trúc dữ liệu đặc biệt mà Cuckoo gọi là Global Container. Container này chỉ đơn giản là một từ điển Python lớn, bao gồm các kết quả trừu tượng được tạo ra bởi tất cả các module được phân loại theo khóa nhận dạng của chúng.

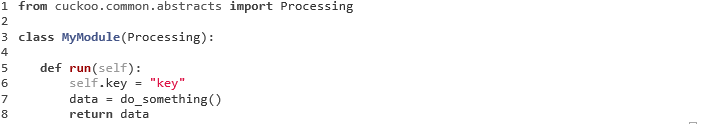
Lưu ý đối với mỗi module mới được thêm vào ta phải khai báo một vùng chuyên dụng trong file config của processing module ở đường dẫn cuckoo/conf/processing.conf. Ví dụ nếu bạn viết một module mới có tên mymodule.py (cuckoo/processing/mymodule.py) thì ta thêm vào file processing.conf như sau.



Một vài processing module mặc định:

* Memory (cuckoo/processing/memory.py): thực thi Volatility để dump toàn bộ memory.
* NetworkAnalysis (cuckoo/processing/network.py) : phân giải các file PCAP để lấy thông tin như lưu lượng DNS, domain, IP, HTTP request, IRC và lưu lượng SMTP.
* StaticAnalysis (cuckoo/processing/static.py): thực hiện phân tích tĩnh các file PE32.
* Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/processing/>

Để tạo một module mới trong Processing, ta phải đặt module ấy trong đường dẫn cuckoo/processing/ theo cấu trúc sau:



Mỗi processing module nên chứa các thông tin sau:

* MyModule: tên class thừa kế từ Processing.
* Run(): tên hàm thực thi.
* Self.key: dùng để xác định tên được sử dụng như một sub container cho dữ liệu trả về.
* Một tập dữ liệu (danh sách, từ điển, chuỗi,…) dùng để chèn vào sau global container.

1.4.4. Reporting Modules:

Sau khi kết quả thô trả về được xử lý bởi các processing module và được trừu tượng hóa, vùng Global Container đã được tạo ra và được Cuckoo chuyển qua Reporting module khả dụng để xử lý, nơi sẽ chuyển các kết quả trả về ấy có thể xem được ở những format khác nhau.

Tất cả Reporting module cần được đặt trong đường dẫn cuckoo/cuckoo/reporting/. Đồng thời phải khai báo các module này trong file reporting.conf ở đường dẫn /cuckoo/conf/reporting.conf (giống với cách khai báo của processing module trong file processing.conf).

Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/reporting/>

1.4.5. Analysis Packages:

Analysis Package là các core component của Cuckoo Sandbox. Chúng bao gồm các class Python mô tả cách thức các component analyzer (bộ phân tích) của Cuckoo quản lý các thủ tục phân tích đối với một file đã cho trong môi trường máy guest.

Cuckoo cung cấp một vài analysis package mặc định, tuy nhiên bạn cũng có thể tự tạo mới hoặc sửa đổi một package đã có.

Danh sách các package tồn tại theo thứ tự bảng chữ cái: applet, bin, cpl, dll, doc, exe, generic, ie, js, jar, msi, pdf, ppt, psl, python, vbs, wsf, xls, zip.

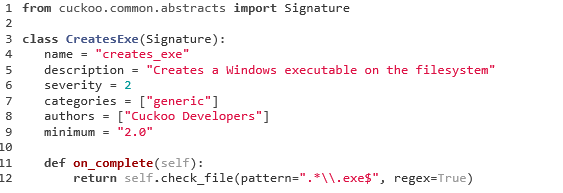
Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/packages/>

1.4.6. Signatures:

Với Cuckoo Sandbox, bạn có thể tạo các signature để có thể so sánh với kết quả phân tích để xác định một số mẫu có sẵn, các mẫu này vốn đại diện cho một hành vi độc hại nào đó hoặc một hành vi mà bạn quan tâm.

Điều này làm đơn giản hóa việc giải thích kết quả cũng như để xác định tự động các mẫu phần mềm độc hại được quan tâm.

Để tạo một signature ta chỉ cần đặt nó vào đường dẫn cuckoo/cuckoo/signatures/ . Sau đây là ví dụ:



Các thông tin cần khai báo:

* Name: Định danh của signature.
* Description: Mô tả của signature sắp tạo.
* Severity: Xác định mức độ nghiêm trọng (thường từ 1 đến 3).
* Categories: Danh sách các danh mục mô tả loại sự kiện trùng khớp.
* Families: Danh sách tên các họ malware, trong trường hợp là known malware.
* Authors: Danh sách tên tác giả tạo signature này.
* References: Danh sách các URL để định nghĩa signature.
* Enable: Bật/Tắt(False) signature.
* Alert: Dùng để xác định signature nên được report.
* Minium: Phiên bản tối thiểu của Cuckoo cần để chạy thành công signature này.
* Maximum: Phiên bản tối đa của Cuckoo để chạy thành công signature này.

Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/customization/signatures/>

II. Cài đặt và cấu hình Cuckoo Sandbox:

2.1.Cài đặt trên máy host:

Chắc chắn rằng hệ thống đã được cập nhật:

$ sudo apt-get remove apt-listchanges

$ sudo apt-get update && sudo apt-get upgrade -y && sudo apt-get upgrade -y && sudo apt-get dist-upgrade -y && sudo apt-get autoremove -y

Cài đặt các thư viện **Python**:

$ 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 libjansson-dev libmagic-dev

Để sử dụng **Danjo-based** web interface, hệ cơ sở dữ liệu **MongoDB** cần được cài:

$ sudo apt-get install mongodb

Cài đặt **Virtual Box** (có thể chọn **VMWARE**):

$ echo deb http://download.virtualbox.org/virtualbox/debian xenial contrib | sudo tee -a /etc/apt/sources.list.d/virtualbox.list

$ wget -q https://www.virtualbox.org/download/oracle\_vbox\_2016.asc -O- | sudo apt-key add -

$ sudo apt-get update

$ sudo apt-get install virtualbox-5.1

Cài đặt **Tcpdump**:

* Do trên Ubuntu AppAmor được mặc định bật sẵn nên sẽ không thể ghi các file vào các thư mục có ký tự “.” bắt đầu, do đó để lưu được file pcap sau khi phân tích ta phải cài đặt AppArmor utilities và disable AppAmor đi:

$ sudo apt-get install tcpdump apparmor-utils

$ sudo aa-disable /usr/sbin/tcpdump

* Cài đặt tcpdump:

$ sudo apt-get install tcpdump

* Tcpdump yêu cầu quyền root nhưng nếu bạn không muốn tcpdump chạy với quyền root, bạn sẽ phải cài đặt cụ thể các khả năng bằng lệnh setcap và getcap:

$ sudo setcap cap\_net\_raw,cap\_net\_admin=eip /usr/sbin/tcpdump

$ getcap /usr/sbin/tcpdump

/usr/sbin/tcpdump = cap\_net\_admin,cap\_net\_raw+eip

* Nếu setcap chưa được cài đặt: $ sudo apt-get install libcap2-bin
* Nếu setcap không hoạt động chạy lệnh sau: $ sudo chmod +s /usr/sbin/tcpdump

Cài đặt **Volatility** để dump memory:

$ sudo apt install git

$ git clone https://github.com/volatilityfoundation/volatility.git

$ cd /home/your\_username/volatility

$ sudo python setup.py install

Cài đặt các plugin của **Volatility**:

* **Distorm3**:

Download Distorm3: <https://github.com/gdabah/distorm/releases>

$ cd /home/YourUserName/Downloads

$ tar -xvzf distorm-3.x.x.tar.gz // x.x là phiên bản bạn đã download

$ cd /home/YourUserName/Downloads/distorm-3.x.x

$sudo python setup.py install

* **Yara**:

$ sudo apt-get install autoconf

$ sudo apt-get install libtool-bin

Download Yara: https://github.com/VirusTotal/yara/releases

$ cd /home/YourUserName/Downloads

$ tar -xvzf yara-3.x.x.tar.gz

$ cd /home/YourUserName/Downloads/yara-3.x.x

$ ./bootstrap.sh

$ ./configure --with-crypto --enable-magic --enable-cuckoo

$ make

$ sudo make install

$ sudo -H pip install yara-python

* **PyCrypto**:

Download PyCrypto: https://pypi.python.org/pypi/pycrypto

$ cd /home/YourUserName/Downloads

$ tar -xvzf pycrypto-2.x.x.tar.gz

$ cd /home/YourUserName/Downloads/pycrypto-2.x.x

$ python setup.py build

$ sudo python setup.py install

* **Openpyxl**:

$ sudo -H pip install openpyxl

* **UJSON**:

$ sudo -H pip install ujson

* **Ipython**:

$ sudo -H pip install jupyter

Cài đặt **Cuckoo Sandbox**:

* Thêm user mới có tên cuckoo:

$ sudo adduser cuckoo

$ sudo usermod -a -G vboxusers cuckoo #thêm user vào group vboxuser

$ sudo usermod -a -G libvirtd cuckoo #thêm vào group chạy module ảo hóa libvirtd

* Cài đặt Cuckoo: (2 Cách)
* Cách 1: Sử dụng pip

$ sudo pip install -U pip setuptools

$ sudo pip install -U cuckoo

Tuy nhiên cuckoo khuyến nghị nên cài đặt cuckoo trong một môi trường python cô lập được gọi là virtualenv vì thế trước khi chạy 2 lệnh trên ta nên cài và khởi động môi trường virtualenv. Do đó các câu lệnh sẽ theo thứ tự sau:

$ [sudo] pip install virtualenv

$ virtualenv venv

$ . venv/bin/activate

(venv) $ sudo pip install -U pip setuptools

(venv) $ sudo pip install -U cuckoo

* Cách 2: Build và install từ source

$ pip download cuckoo

$ pip install Cuckoo-2.0.0.tar.gz

Thư mục làm việc của Cuckoo Sandbox (Cuckoo Working Directory - $CDW):

$ virtualenv venv

$ . venv/bin/activate

(venv) $ cd ~/.cuckoo/

2.2. Cài đặt máy ảo:

Để tạo ra môi trường để tiến hành chạy thử các mẫu, Cuckoo Sandbox đòi hỏi một hoặc nhiều máy ảo trên host machine. Cuckoo Sandbox khuyến khích nên chọn môi trường Windows 7 64bit.

Cách tạo một máy ảo trên Virtual Box: <https://forum.bkav.com.vn/forum/bkav-forum/bkav-contest/29597-huong-dan-tao-may-ao-bang-virtualbox-complete>

Sau khi cài đặt máy ảo thành công ta tiến hành cài đặt những thứ cần thiết trên máy ảo đó:

* Cài đặt Guest Additions - Virtual Box (giống Vmtools - VMWARE):
* Devices > Install Guest Additions…
* Một hộp thoại xuất hiện chọn Install
* Tiến hành cài đặt và Restart lại máy
* Cài đặt Python:
* Download gói cài đặt python: <https://www.python.org/downloads/release/python-2713> /.
* Tiến hành cài đặt gói vừa tải về. Kiểm tra bằng lệnh cmd ( Windows + R > cmd > python).
* Cài đặt thư viện PIL (dùng để chụp screenshot): <http://www.pythonware.com/products/pil/> .
* Tắt Firewall/ User Account Control/ Update.
* Cài đặt các phần mềm thuộc bên thứ 3 (Office, Adobe Reader, Flash…):
* Cài đặt office 2010 (hoặc bất cứ phiên bản nào).
* Cài đặt Adobe Flash Player: https://get.adobe.com/flashplayer/.
* Cài đặt Adobe Reader: https://get.adobe.com/reader/.
* Trên host machine ta tạo một card mạng host ảo có tên vboxnet0 có địa chỉ ip 192.168.56.1:

$ vboxmanage hostonlyif create

$ vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1

$ ifconfig

…

vboxnet0 Link encap:Ethernet HWaddr 0A:00:27:00:00:00

inet addr:192.168.56.1 Bcast:192.168.56.255 Mask:255.255.255.0

inet6 addr: fe80::800:27ff:fe00:0/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:273 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:0 (0.0 b) TX bytes:31818 (31.0 KiB)

* Tiếp theo ta set card mạng của máy ảo thành card hostonly vboxnet1:

$ vboxmanage modifyvm <Ten\_may\_ao> --hostonlyadapter1 vboxnet0

$ vboxmanage modifyvm <Ten\_may\_ao> --nic1 hostonly

* Đặt địa chỉ ip tĩnh trên máy ảo:

Static IP - 192.168.56.101

DNS - any DNS server (8.8.8.8)

Default Gateway - 192.168.56.

* Copy file **agent.py** lên máy ảo và chạy:
* Vào đường dẫn sau trên host machine: /home/YourUserName/.cuckoo/agent/
* Kéo thả file agent.py vào máy ảo vừa tạo.
* Tiến hành chạy file agent.py trên máy ảo.
* Tạo snapshot cho máy ảo vừa tạo (Mỗi khi mẫu thử được Cuckoo đẩy đến máy ảo sẽ dùng snapshot này để khởi động và chạy):

$ vboxmanage snapshot "<Tên\_Máy\_Ảo>" take "<Tên\_snapshot>" –pause

$ vboxmanage controlvm "<Tên\_Máy\_Ảo>" poweroff

$ vboxmanage snapshot "<Tên\_Máy\_Ảo>" restorecurrent

$ vboxheadless --startvm "<Tên\_Máy\_Ảo>"

* Để máy ảo có thể truy cập internet, ta cần thêm một số rule vào iptables để các gói tin được forward đến host và đi internet:

$ iptables -A FORWARD -o eth0 -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

$ iptables -A POSTROUTING -t nat -j MASQUERADE

* Enable IP Forwarding:

$ echo 1 > /proc/sys/net/ipv4/ip\_forward

* Tuy nhiên mỗi khi khởi động lại, card vboxnet0 vừa tạo sẽ không còn do đó ta có thể sử dụng system.service:
* Tạo một bash script để chạy lệnh vboxmanage:

$ sudo mkdir /opt/systemd/

$ nano /opt/systemd/vboxhostonly

#!/bin/bash

vboxmanage hostonlyif create

vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1

Ctrl+X > Y > Enter

* Tiếp theo ta tạo một file vboxhostonly.service trong /etc/systemd/system/ có nội dung sau:

Description=Setup VirtualBox Hostonly Adapter

After=vboxdrv.service

[Service]

Type=oneshot

ExecStart=/opt/systemd/vboxhostonly

[Install]

WantedBy=multi-user.target

* Cài đặt service này và enable nó lúc khởi động:

$ systemctl daemon-reload

$ systemctl enable vboxhostonlynic.service

$ systemctl start vboxhostonlynic.service # kiem tra service

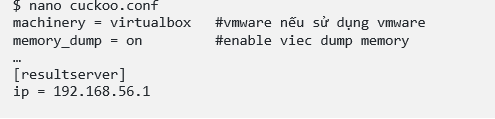
2.3. Cấu hình Cuckoo Sandbox:

Tất cả các file config của Cuckoo Sandbox đều nằm trong đường dẫn **$CWD/conf**/:

(venv)$ cd ~/.cuckoo/conf/

2.3.1. cuckoo.conf:

Tập tin cuckoo.conf chứa các tùy chọn cấu hình chung.



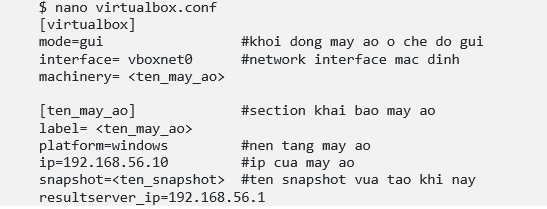
2.3.2. auxiliary.conf:

Tập tin auxiliary.conf chứa các định nghĩa các tùy chọn của các modue Auxiliary.



2.3.3. virtualbox.conf/vmware.conf (machinery config)

Tập tin virtualbox.conf định nghĩa cách Cuckoo tương tác với phần mềm ảo hóa Virtualbox.

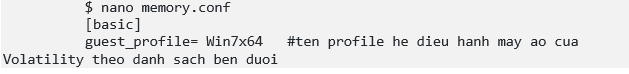


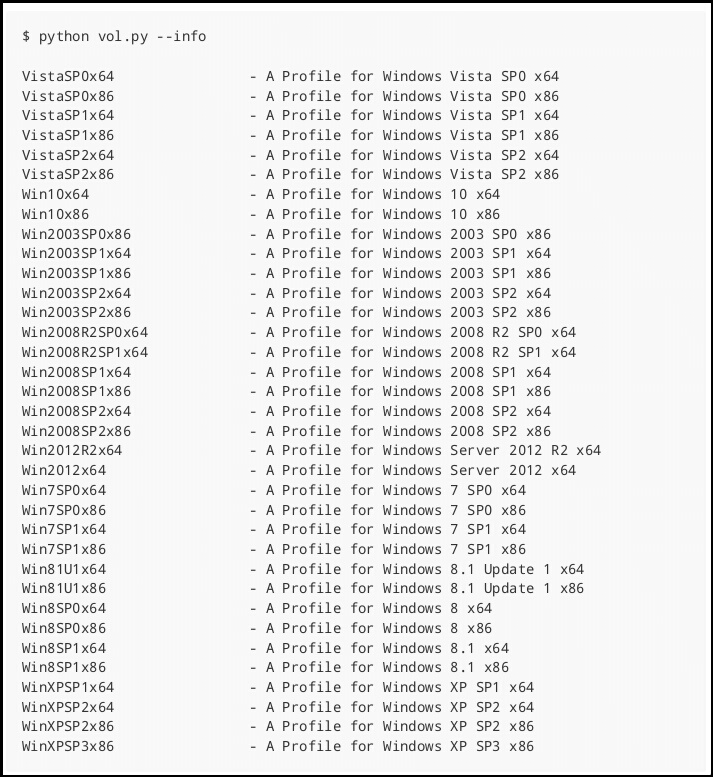
2.3.4.processing.conf:

Tập tin processing.conf cho phép enable/disable cấu hình của các module processing và xác định cách thức xử lý dữ liệu thô thu thập được trong quá trình phân tích.

2.3.5.memory.conf:

Tập tin memory.conf cho phép bật tắt các plugin dùng để phân tích memory dump của volatility.





Hình 4: Tên Profile của Volatility

2.3.6. reporting.conf:

Tập tin reporting.conf cho phép enable/disable các định dạng báo cáo mà Cuckoo Sandbox có thể xuất ra (JSON, pdf, DB…).

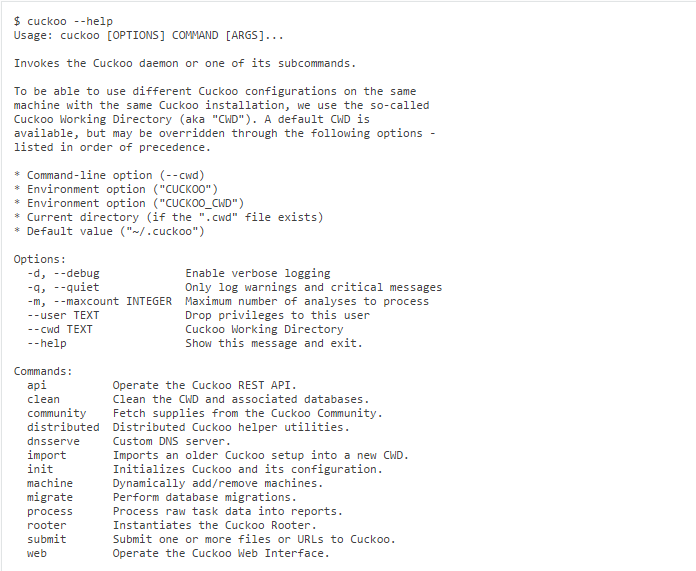


III. Sử dụng:

3.1.Khởi động Cuckoo Sandbox:

Sau khi quá trình cài đặt thành công, ta tiến hành chạy Cuckoo Sandbox lần đầu tiên.

$ cuckoo --help #hien thi danh sach cac option va api



Hình 5: Lệnh và các option của cuckoo.

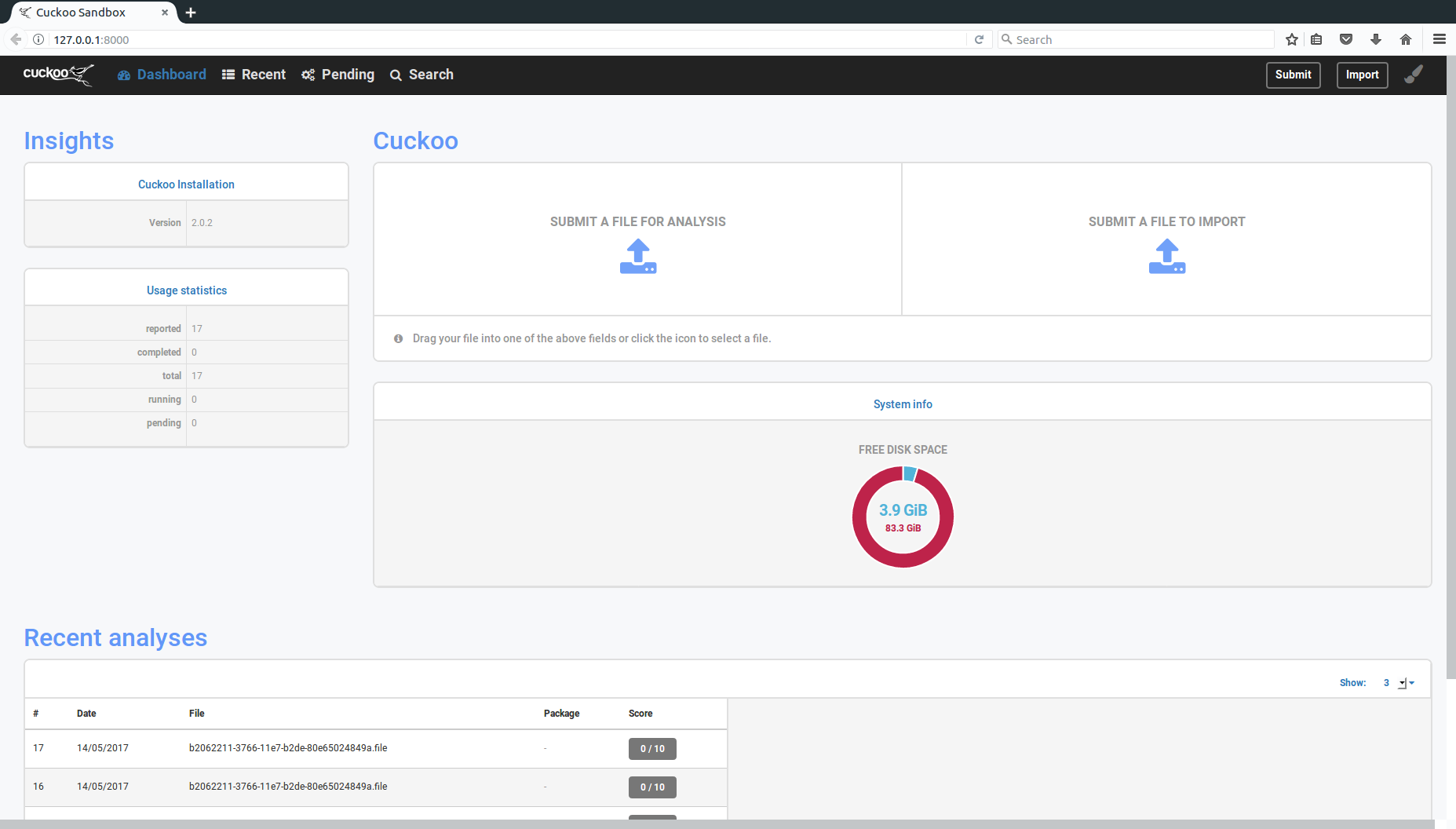
Tuy nhiên trước khi khởi động ta cần download các signature miễn phí của cuckoo sandbox. Đây là tập 300 signature đại diện cho các hành vi nguy hiểm giúp đơn giản hóa kết quả cuối cùng.

$ cuckoo community #tự động fetch tệp signature từ server của cuckoo

(hoặc) $ cuckoo community --file your\_file.tar.gz #chi dinh tep chu ky co san

Khởi động web interface (mặc định được chạy tại port 8000):

$ cuckoo web runserver

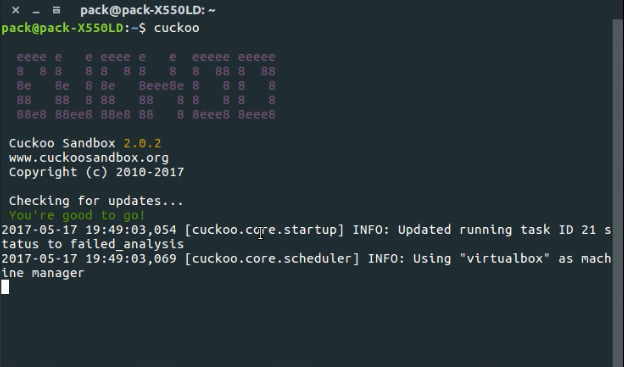


Hình 6: Giao diện web Cuckoo Sandbox

Khởi động Cuckoo Sandbox:

$ cuckoo

Hoặc $ cuckoo --cwd ~/.cuckoo/ #de chi ro duong dan cua cuckoo



Hình 7: Khởi động Cuckoo Sandbox

3.2.Thực hiện submit mẫu thử:

Để thêm mẫu thử vào Cuckoo Sandbox có 2 cách.

**Cách 1** thông qua dòng lệnh với option submit:

$ cuckoo submit /path/to/binary #submit binary file

$ cuckoo submit --url http://www.example.com #submit url

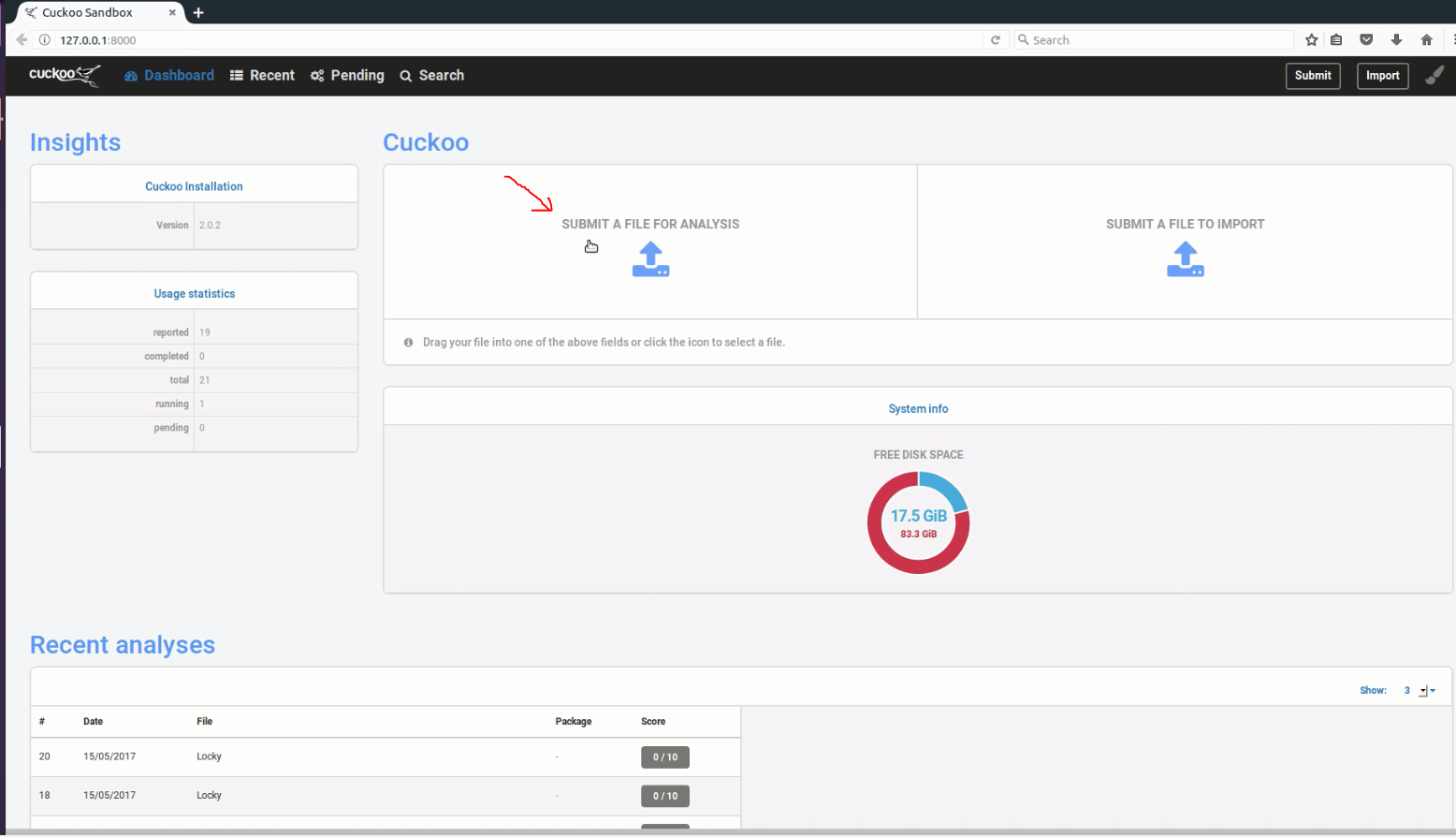
$ cuckoo submit --priority 5 /path/to/binary #tuy chinh do uu tien

$ cuckoo submit --timeout 60 /path/to/binary #thoi gian timeout

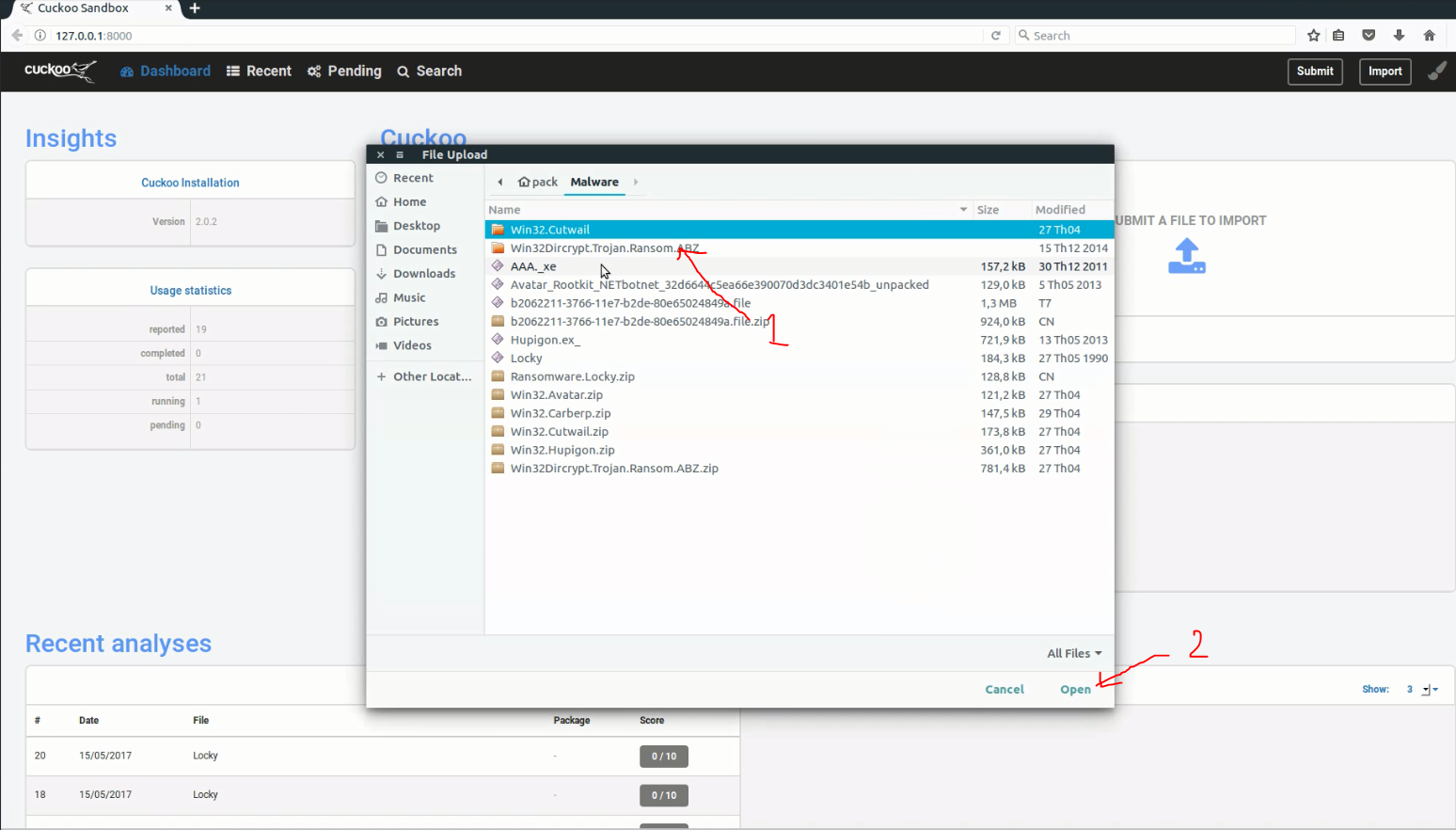
Tham khảo thêm: <http://docs.cuckoosandbox.org/en/latest/usage/submit/>

**Cách 2** thông qua giao diện web:

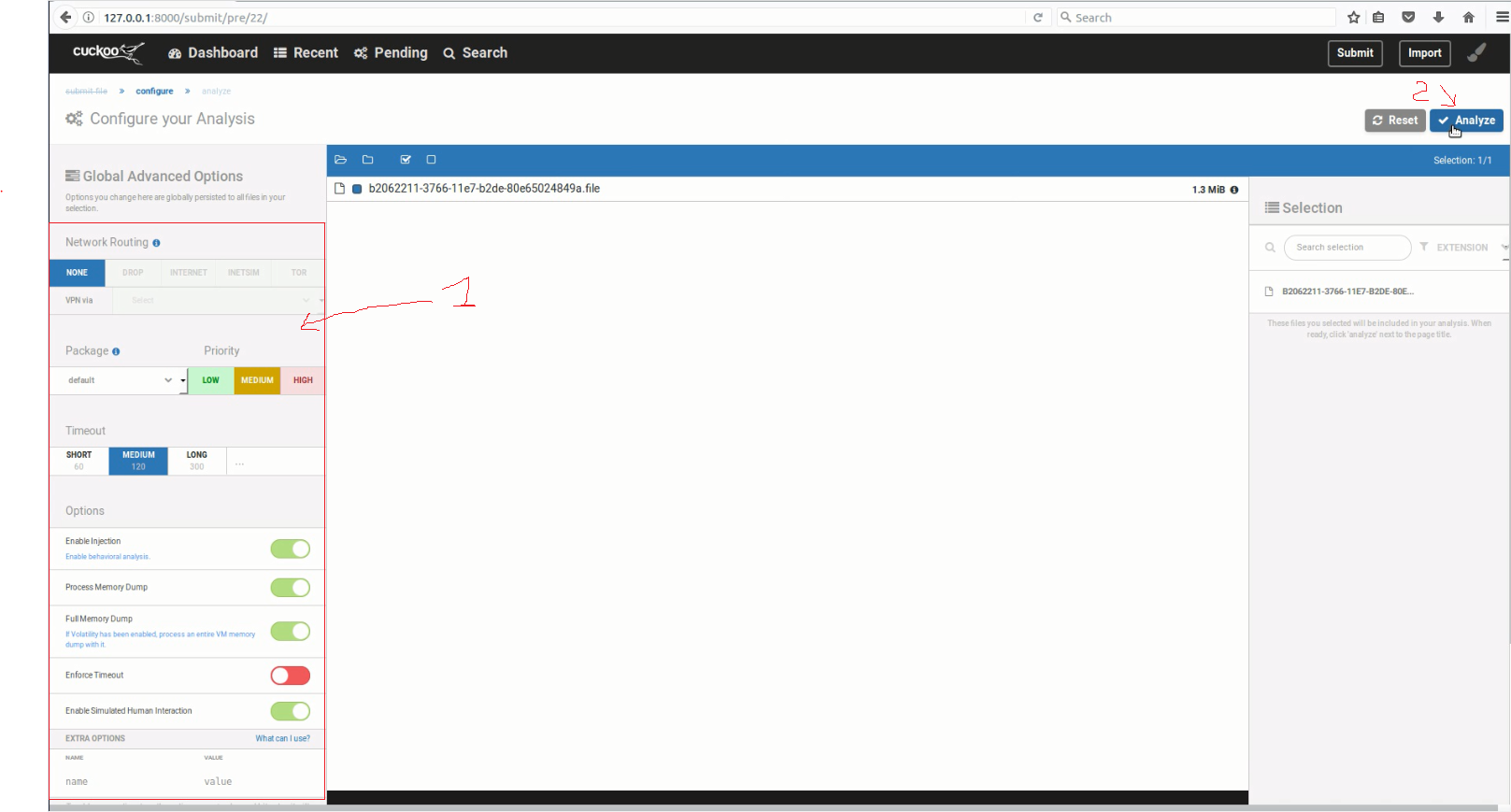
* Từ giao diện web chọn “Submit A File For Analysis”:



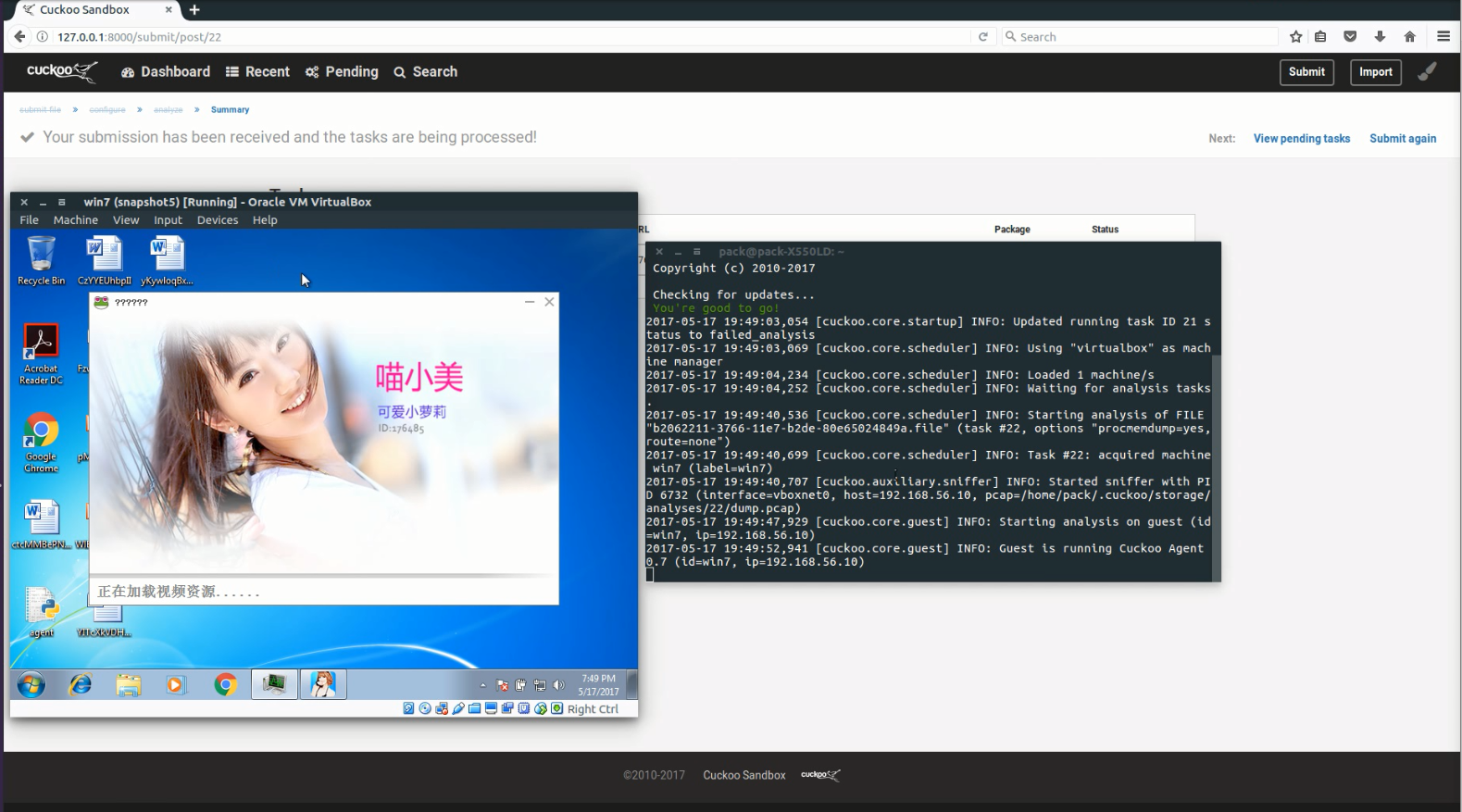
* Sau đó chọn file cần phân tích và nhấn “Open”



* Cuối cùng ta tùy chỉnh các thông số cho 1 phiên phân tích
* Network Routing: Thiết lập kết nối như VPN, hoặc proxy Tor.
* Package: Chọn loại package (exe, pdf,…).
* Priority: Độ ưu tiên (LOW/MEDIUM/HIGH).
* Timeout: Thiết lập thời gian chờ cho phiên phân tích.
* Enable Injection: Enable/Disable phân tích hành vi.
* Process Memory Dump: Dump memory của từng process.
* Full Memory Dump: Dump toàn bộ memory.
* Enforce Timeoutt: Thi hành thời gian chờ.
* Enable Simulated Human Interaction: Mô phỏng tương tác của người dùng.

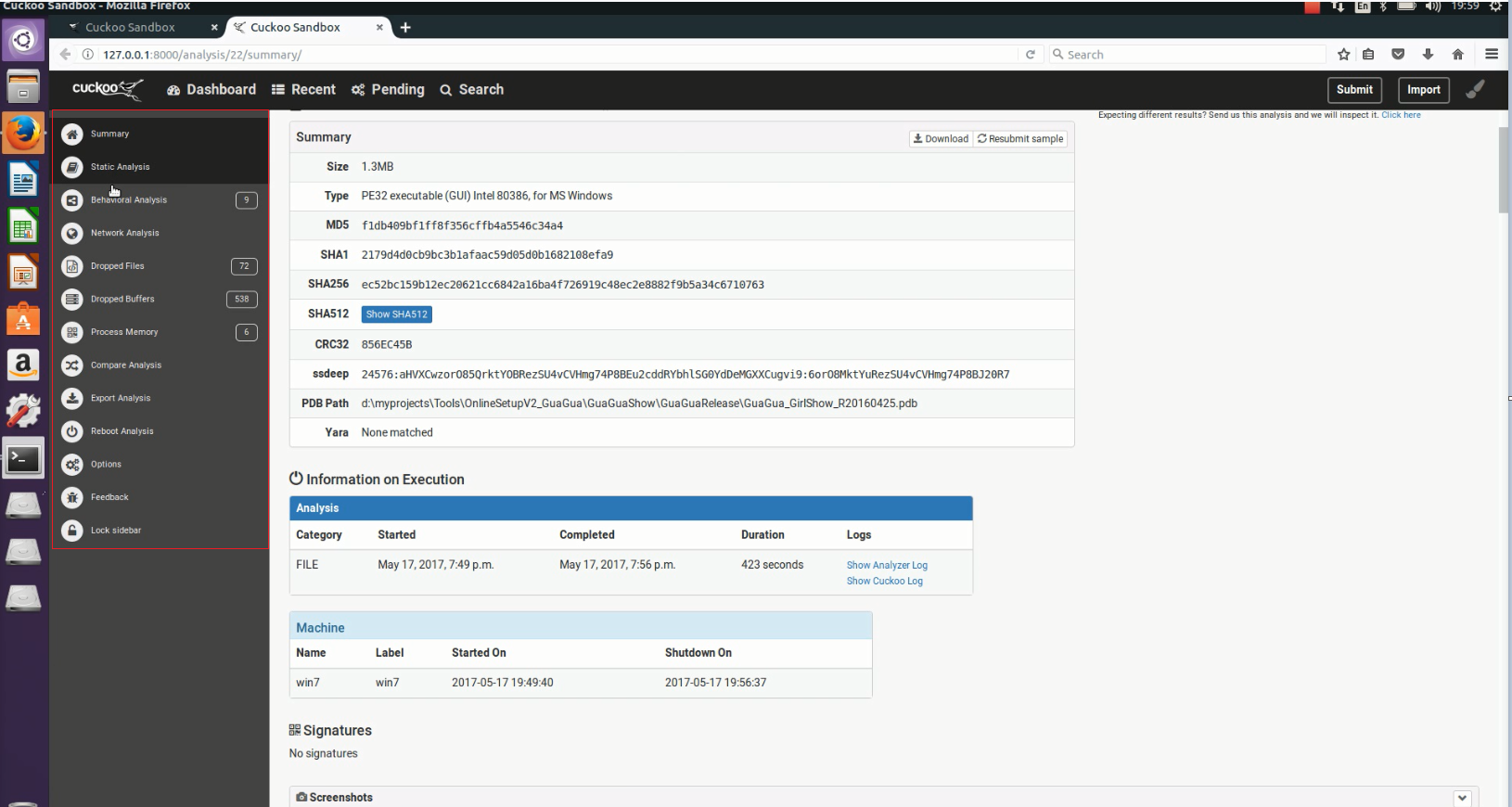


* Sau khi hoàn tất các thủ tục submit, các module được load và bắt đầu một phiên phân tích:



3.3.Các kết quả được report:

Sau khi phiên phân tích kết thúc thành công, các báo cáo sẽ được xử lý và trình bày theo từng phần ở sidebar bên trái.

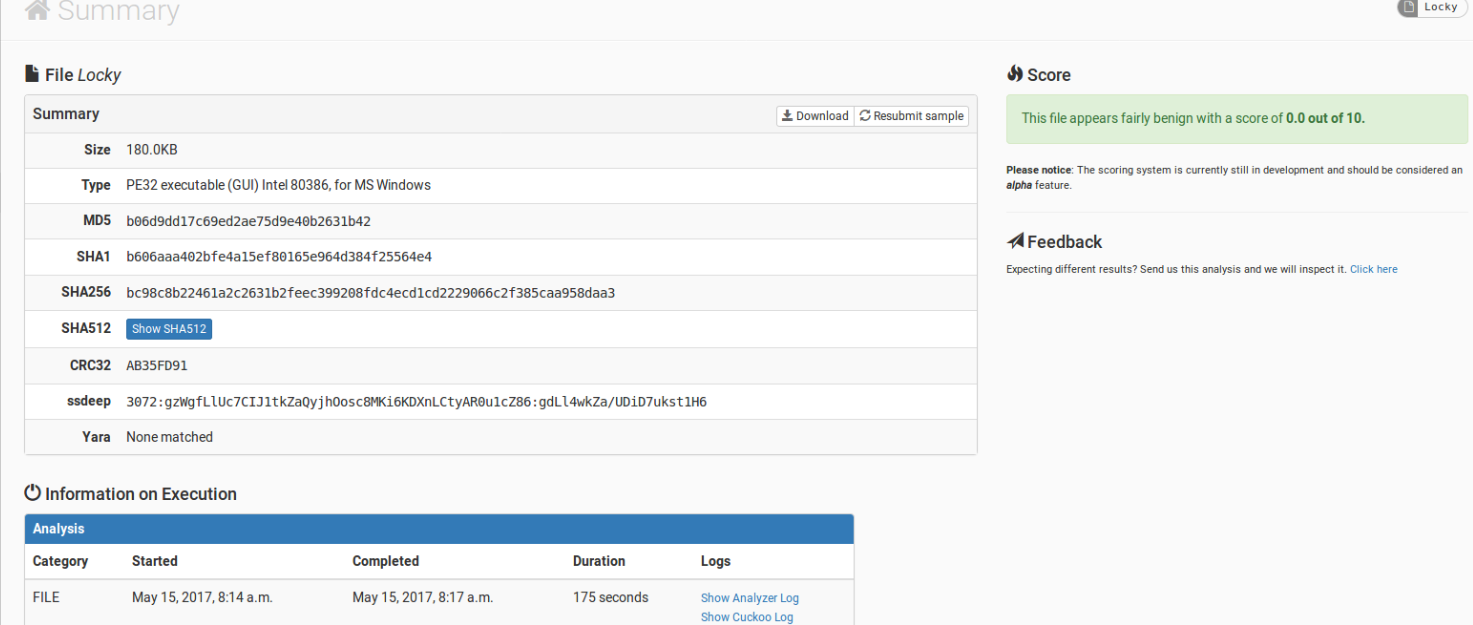


Hình 8: Kết quả được chia theo từng section.

3.3.1. Summary

Đây là báo cáo tóm lược về file vừa phân tích. Các báo cáo tóm lược bao gồm:

* Summary: cho biết loại tệp tin, kích thước, mã hash (md5, sha1), ssdeep hash (fuzzy hash), đường dẫn của file PDB (Program Database) và Yara signature.
* Information on Execution: cho biết định dạng tệp, thời gian bắt đầu và kết thúc phiên phân tích, thời gian diễn ra (duration) và các file log khi chạy phiên phân tích này.
* Machine: cho biết thông tin về máy guest sử dụng để phân tích.
* Signatures: cho biết các hành động theo 3 mức độ: low (xanh), medium (vàng), high (đỏ). Các hành động này được phát hiện dựa trên các signature community của cuckoo mà chúng ta đã tải về.
* Screenshots: hình ảnh của máy guest lúc thực thi tệp.
* Cuối cùng là tên các host, địa chỉ ip mà tệp này thực hiện các truy vấn đến.

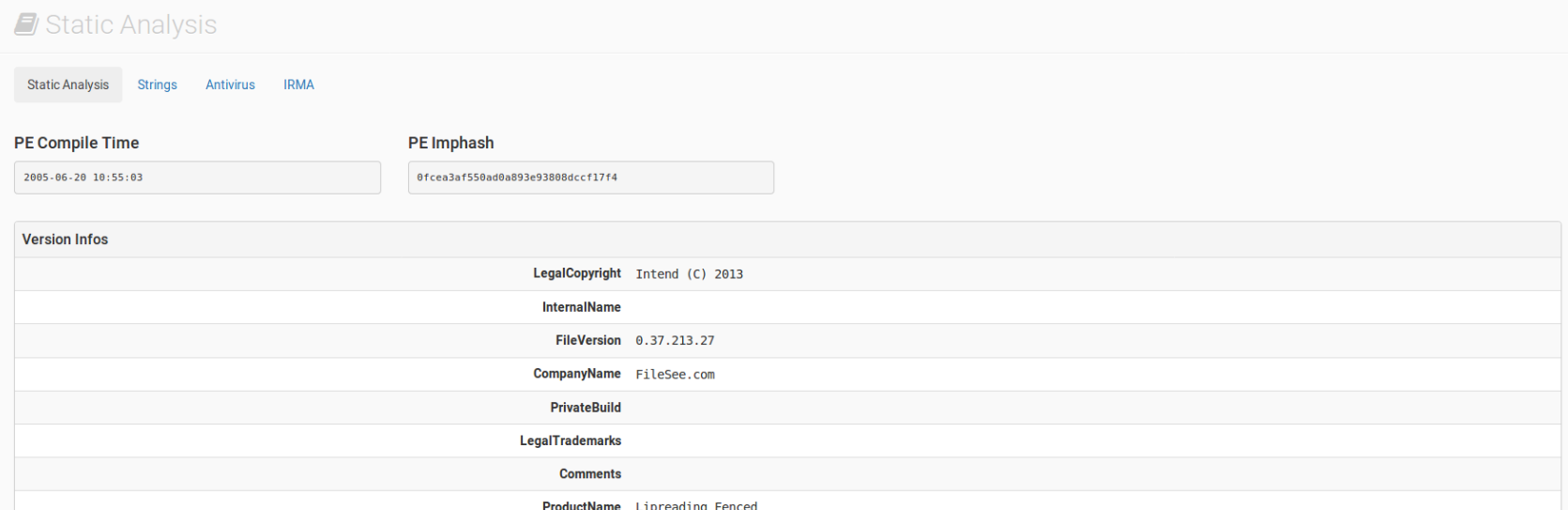


Hình 10: Báo cáo Summary

3.3.2. Static Analysis

Đây là báo cáo chi tiết về việc phân tích tĩnh tệp tin.

* Static Analysis: Cho biết các thư viện đã import/system calls.
* String: Liệt kê các chuỗi xuất hiện trong tệp.
* Antivirus: Kết quả quét tệp với các Antivirus khác nhau.



Hình 10: Báo cáo Static Analysis.

3.3.3. Behavioral Analysis

Đây là báo cáo về hành vi của tệp tin khi thực thi.

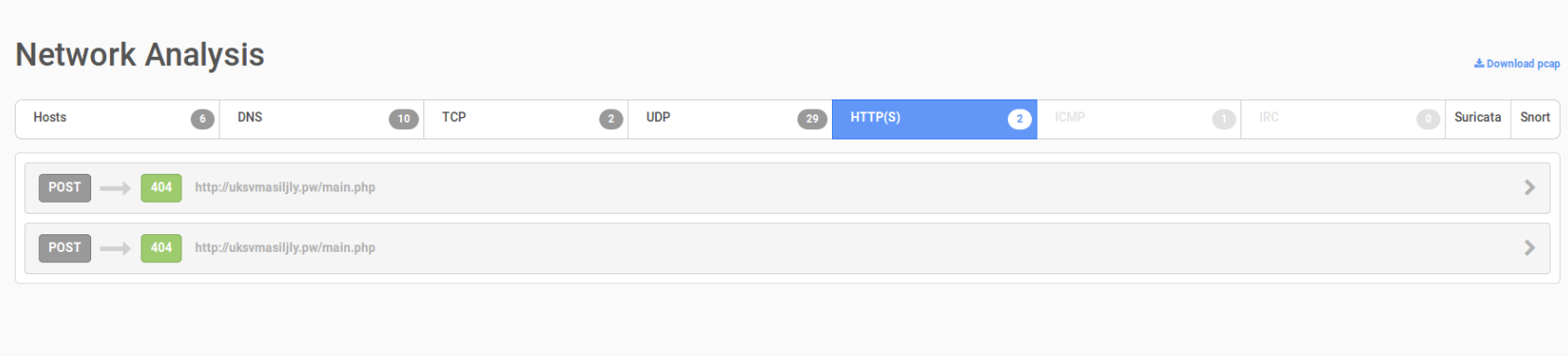
* Process Tree: liệt kê các process sinh ra trong quá trình thực thi theo sơ đồ cây.
* Theo dõi các hàm api mà từng process đã gọi, status (SUCCESS/FAIL) khi gọi api này, giá trị trả về (return) của hàm api và số lần lập lại (Repeat).



Hình 11: Báo cáo Behaviral Analysis.

3.3.4. Network Analysis

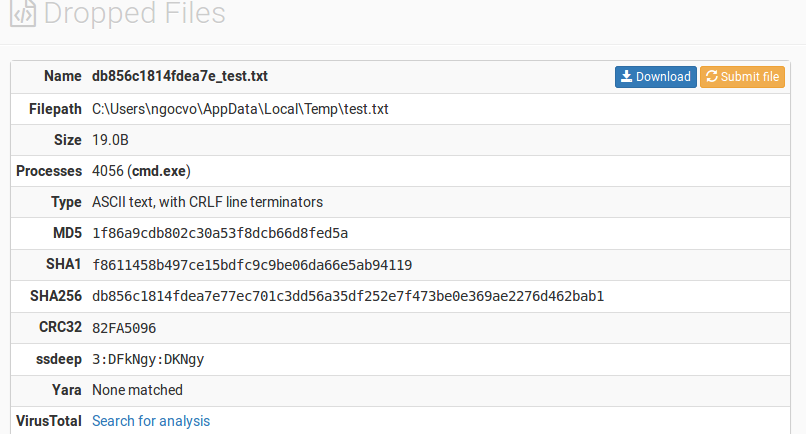
Đây là báo cáo chi tiết các request mạng mà tệp tin đã gửi đi và các response trả về bao gồm chi tiết các gói tin UDP, TCP; các query DNS; các kết nối HTTP(s) và tên các Hosts kết nối đến



Hình 12: Báo cáo Network Analysis

3.3.5. Dropped Files/ Dropped Buffers:

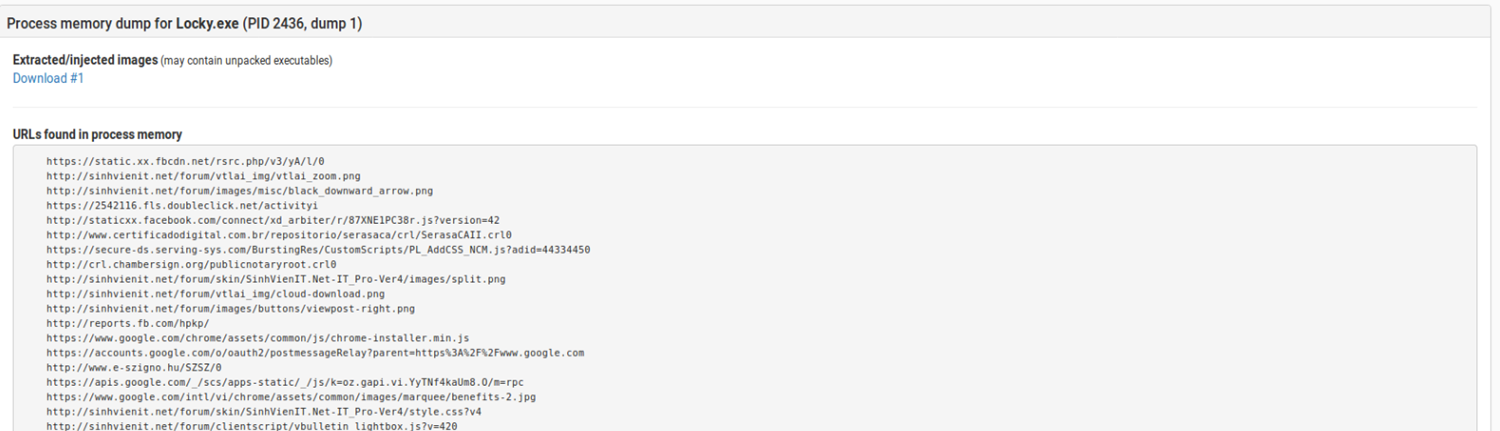
Đây là báo cáo về các tệp tin/vùng nhớ tạm đã được tệp thực thi tạo ra. Ở từng file ta có thể quét signature với VirusTotal hoặc Submit và phân tích riêng đối với từng file.



Hình 13: Báo cáo Dropped Files.

3.3.6. Process Memory:

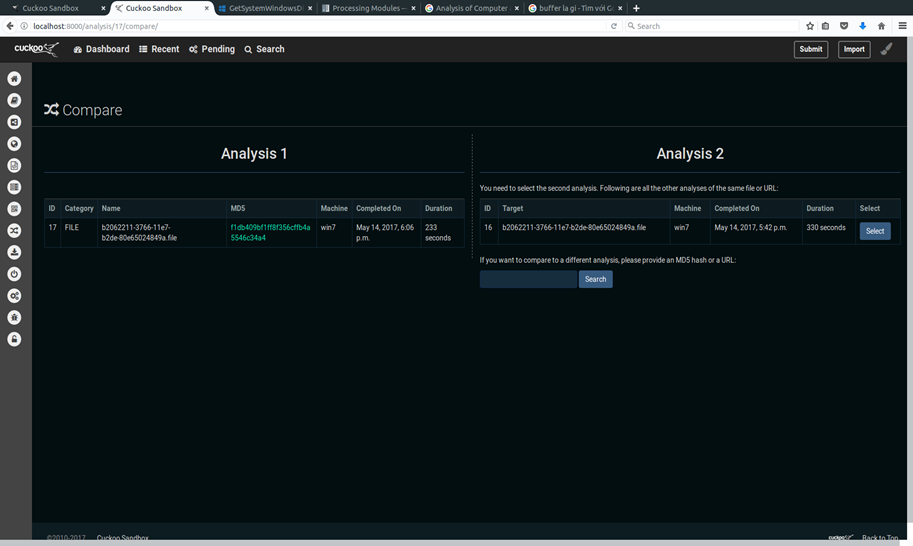
Đây là báo cáo về các process memory dump. Mỗi process được sinh ra trong quá trình phân tích đều được dump memory. Ở mỗi process memory dump liệt kê PID và các URL được tìm thấy.



Hình 14: Báo cáo Process Memory.

3.3.7. Compare Analysis:

Dùng để so sánh hai kết quả phân tích với nhau.

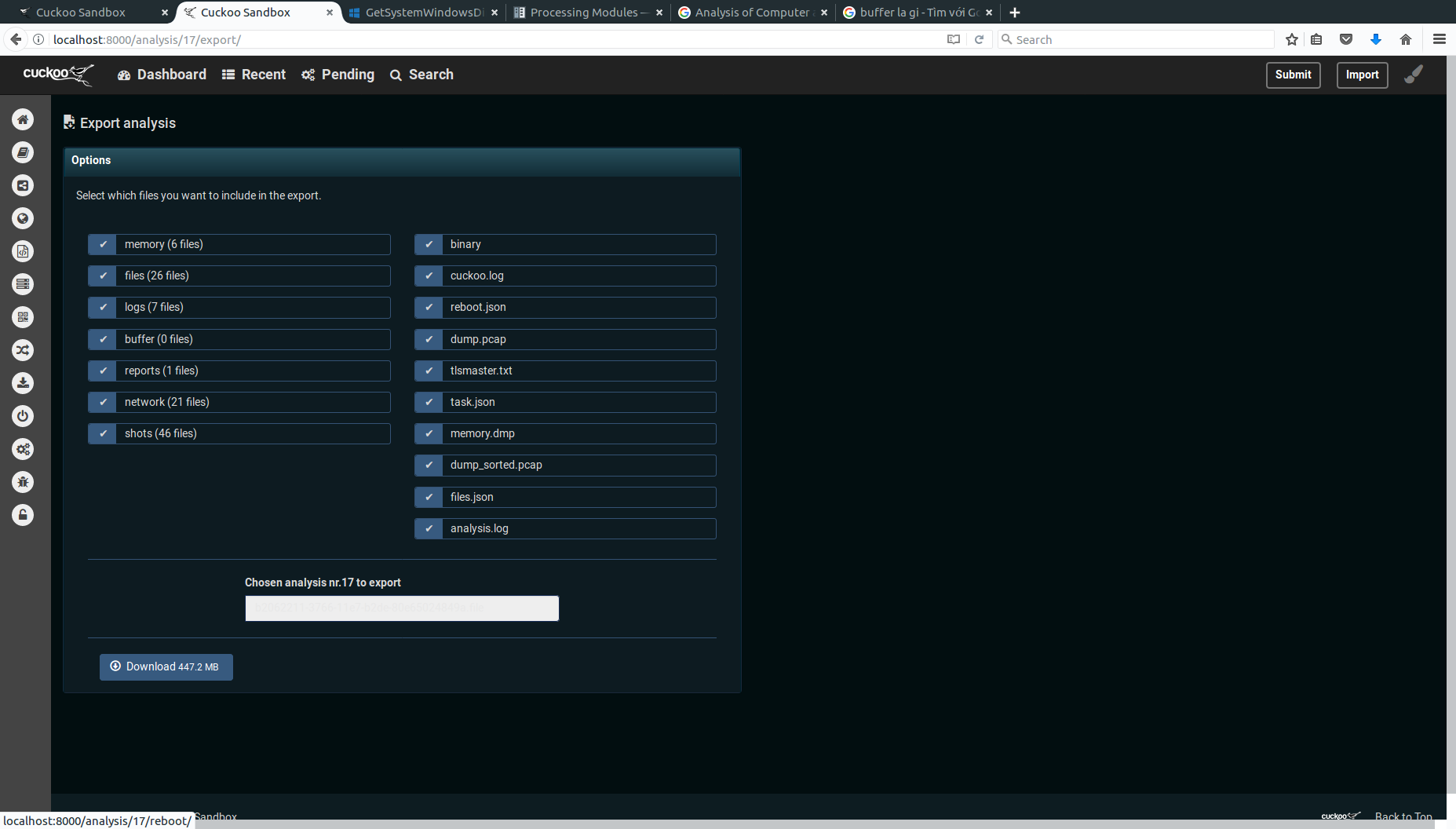


Hình 15: So sánh hai kết quả.

3.3.8. Export Analysis, Reboot Analysis

Export Analysis: cho phép xuất các kết quả báo cáo (có thể tùy chọn các kết quả cần xuất).

Reboot Analysis: Khởi động lại phiên phân tích.



Hình 16: Xuất các kết quả phân tích.

VI. Đánh giá:

6.1. Tích cực:

* Miễn phí.
* Open-Source.
* Được module hóa.
* Mọi thứ đều tự động.
* Tính tùy biến cao.
* Có thể thực hiện phân tích đồng thời.

6.2. Hạn chế:

* Hệ thống chấm điểm hoạt động chưa tốt.

DEMO: <https://www.youtube.com/watch?v=VHB6oNV9pTA&feature=youtu.be>

PROJECT’S SOURCE CODE: <https://drive.google.com/file/d/0B6RGdSgstKqiY0lGUHRXSGxGajA/view>

TÀI LIỆU THAM KHẢO: <http://docs.cuckoosandbox.org/en/latest/>

--------------------------------------------------------Hết--------------------------------------------------------