



CUCKOO SANDBOX

Análisis Automatizado De Malware



VLADISLAV STELMAKH
U0257580

ÍNDICE

¿Qué es Cuckoo Sandbox? -----	3
Un poco de historia -----	3
Funcionamiento -----	3
Aplicaciones -----	3
Casos de uso -----	4
Arquitectura -----	4
Instalación -----	5

¿Qué es Cuckoo Sandbox?

Cuckoo Sandbox es un sistema de análisis automatizado de malware. Es además, un software gratuito de código abierto (free open source software).

Un poco de historia

Cuckoo Sandbox comenzó como un proyecto “Google Summer of Code”, como parte del proyecto de “The Honeynet” gracias a su fundador y desarrollador Claudio Guarnieri en 2010.

El 5 de febrero de 2011 se anunció y publicó la primera versión beta de Cuckoo Sandbox, y durante este mismo año, Alessandro Tanasi se unió al proyecto, con lo que más tarde aparecería la primera versión estable 0.2 y se anunciaría la 0.3

En 2012 se abrió malwr.com, una instancia pública de Cuckoo Sandbox. También ganaron la primera ronda del programa Magnificent7. A mediados de año, Jurriaan Bremer se unió al equipo, enfocado en la refactorización del componente de análisis de Windows, mejorando la calidad del análisis. A finales de año, se anunciaron las versiones 0.4 y 0.5.

Durante los próximos años, 2013 y 2014, seguirían anunciándose nuevas versiones, para a continuación, en 2015, comenzar a desarrollar un sistema de análisis para Mac OS X.

En 2016 se anunciaría la versión 2.0, con sus variantes RC1 y RC2.

Finalmente, en 2017, anunciarían la versión 2.0.0 que simplificada mucho el uso, mantenimiento, habilidad de actualización, estabilidad... de Cuckoo. Y sobre todo, crearían su propia página web.

Funcionamiento

El funcionamiento de Cuckoo está basado en que le puedes pasar cualquier archivo sospechoso, y él, al cabo de un pequeño período de tiempo, te devolverá un informe detallado donde se especificará el “comportamiento” del archivo durante su ejecución dentro de un S.O. aislado.

Aplicaciones

- Analizar cualquier tipo de archivo malicioso (documentos, pdfs, ejecutables...) e incluso cualquier página web maliciosa.
- Rastrear/comprobar cualquier tipo de llamadas realizadas por todos los procesos generados por el malware.
- Archivos creados, eliminados y descargados por el malware durante su ejecución.
- Hacer un volcado de memoria de los procesos de malware, o un volcado de memoria completa de las máquinas.
- Analizar el tráfico de una red en formato PCAP, incluso existiendo encriptación de por medio (SSL/TLS).
- Capturas de pantalla tomadas durante la ejecución del malware.
- Realizar análisis de memoria avanzados de sistemas virtuales.

Casos de uso

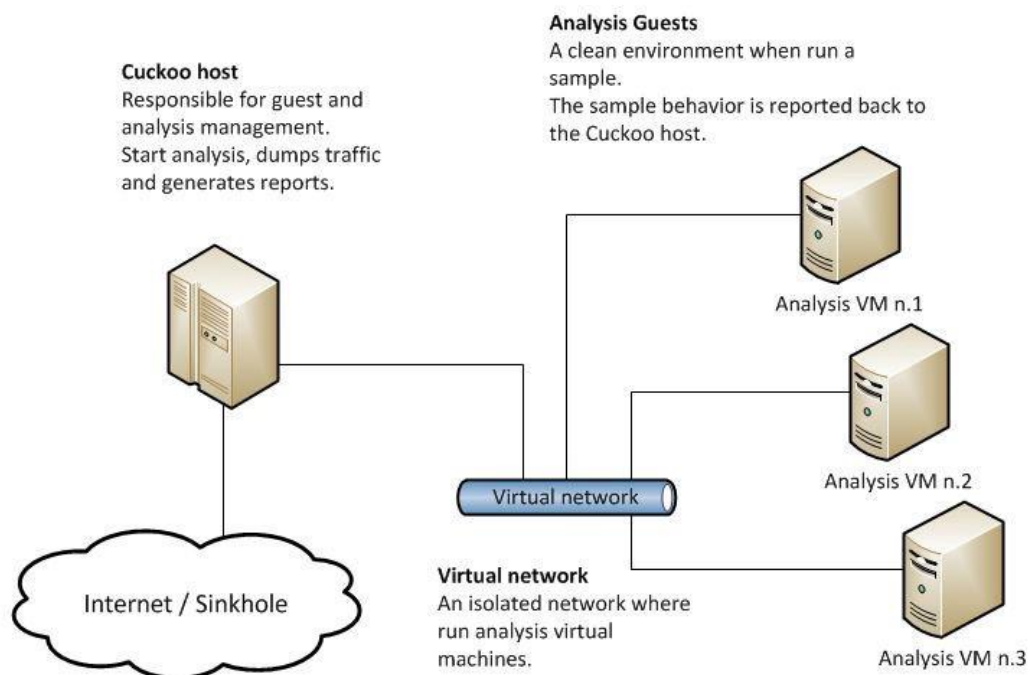
Debido a que Cuckoo tiene un diseño modular, puede ser utilizado tanto como una aplicación independiente como integrarse en marcos más grandes.

Puede utilizarse para analizar:

- Documentos PDF
- Archivos DLL
- Scripts PHP
- Archivos JAR de Java
- Archivos de Python
- Archivos CPL
- URLs y archivos HTML
- Ejecutables genéricos de Windows

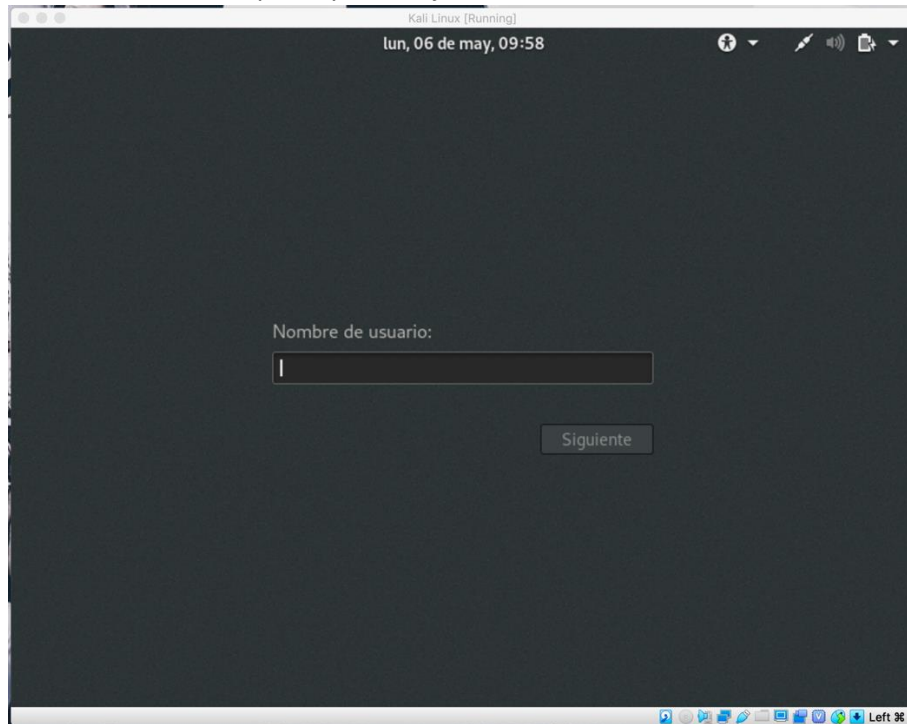
Arquitectura

1. Cuckoo Sandbox es un software de administración central que maneja la ejecución y el análisis de muestras.
2. Cada análisis se inicia en una máquina virtual o física nueva y aislada.
3. Los componentes principales de la infraestructura de Cuckoo son una máquina Host (el software de administración) y una cantidad de máquinas Guest (máquinas virtuales o físicas para análisis).
4. El Host ejecuta el componente central del recinto de seguridad que administra todo el proceso de análisis, mientras que los invitados son los entornos aislados donde las muestras de malware se ejecutan y analizan de forma segura.



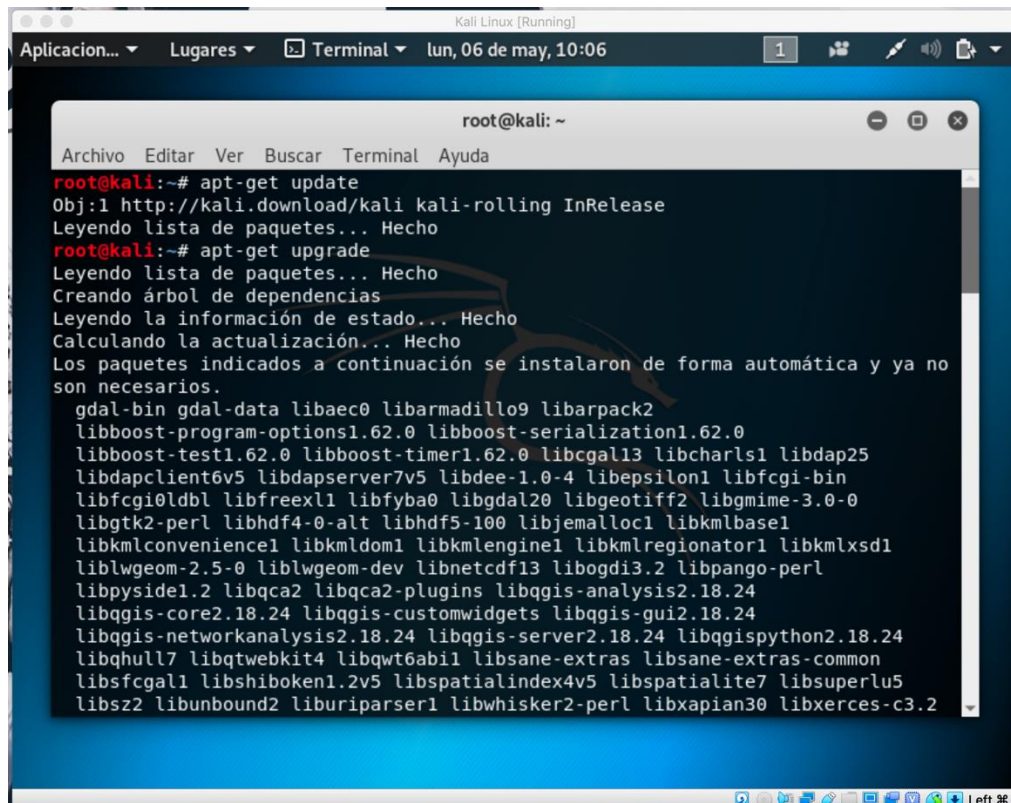
Instalación

Antes de comenzar con la instalación de Cuckoo Sandbox, he instalado previamente una máquina virtual Kali, sobre la que voy a trabajar:



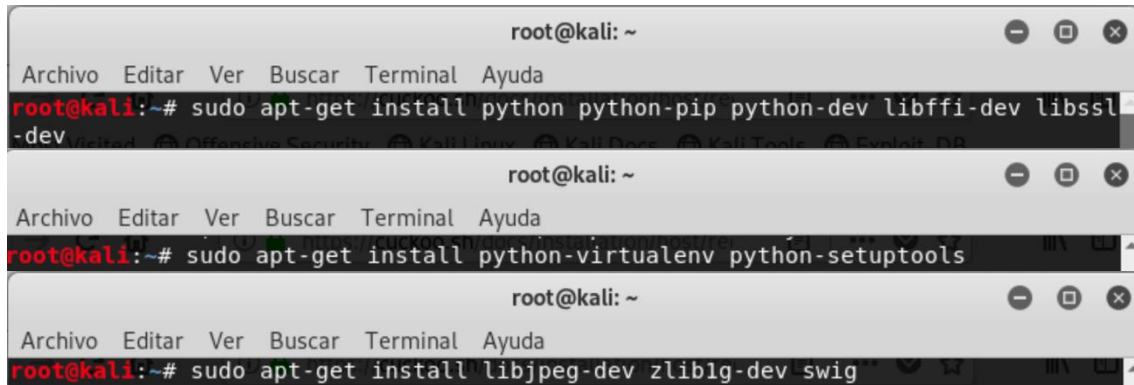
Lo primero que ha sido es ejecutar los siguientes dos comandos para tener todo actualizado:

- apt-get update
- apt-get upgrade



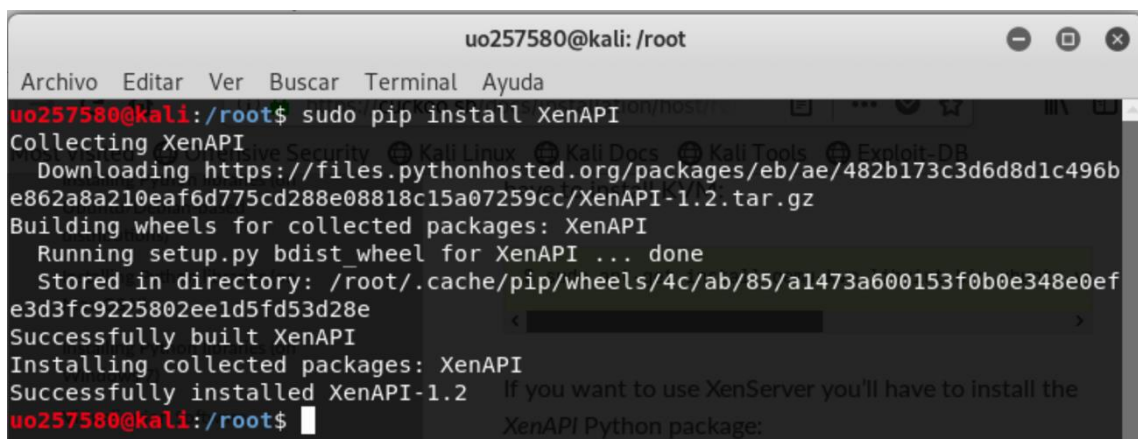
Una vez tenemos Kali totalmente actualizado, previamente a la instalación de Cuckoo Sandbox, hay una serie de prerequisites que debemos cumplir:

- Instalar las librerías de 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`



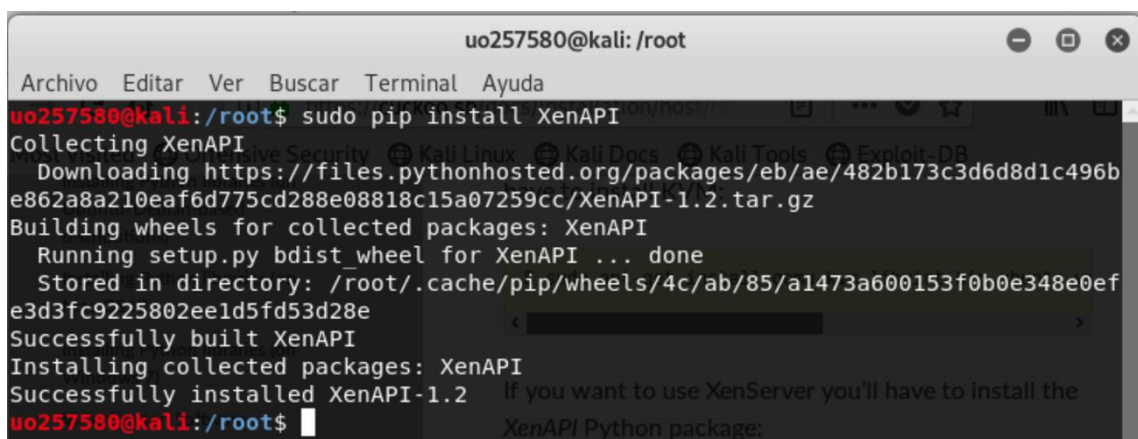
The image shows three terminal windows stacked vertically, each with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a title bar (root@kali: ~). The first terminal shows the command `sudo apt-get install python python-pip python-dev libffi-dev libssl-dev`. The second terminal shows the command `sudo apt-get install python-virtualenv python-setuptools`. The third terminal shows the command `sudo apt-get install libjpeg-dev zlib1g-dev swig`.

- Instalar PostgreSQL



The image shows a terminal window with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a title bar (uo257580@kali: /root). The terminal output shows the command `sudo pip install XenAPI` being executed. The output includes: `Collecting XenAPI`, `Downloading https://files.pythonhosted.org/packages/eb/ae/482b173c3d6d8d1c496be862a8a210eaf6d775cd288e08818c15a07259cc/XenAPI-1.2.tar.gz`, `Building wheels for collected packages: XenAPI`, `Running setup.py bdist_wheel for XenAPI ... done`, `Stored in directory: /root/.cache/pip/wheels/4c/ab/85/a1473a600153f0b0e348e0ef`, `Successfully built XenAPI`, `Installing collected packages: XenAPI`, `Successfully installed XenAPI-1.2`, and a note: `If you want to use XenServer you'll have to install the XenAPI Python package:`.

- Instalar XenAPI



The image shows a terminal window with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a title bar (uo257580@kali: /root). The terminal output shows the command `sudo pip install XenAPI` being executed. The output includes: `Collecting XenAPI`, `Downloading https://files.pythonhosted.org/packages/eb/ae/482b173c3d6d8d1c496be862a8a210eaf6d775cd288e08818c15a07259cc/XenAPI-1.2.tar.gz`, `Building wheels for collected packages: XenAPI`, `Running setup.py bdist_wheel for XenAPI ... done`, `Stored in directory: /root/.cache/pip/wheels/4c/ab/85/a1473a600153f0b0e348e0ef`, `Successfully built XenAPI`, `Installing collected packages: XenAPI`, `Successfully installed XenAPI-1.2`, and a note: `If you want to use XenServer you'll have to install the XenAPI Python package:`.

- Instalar tcpdump

```

uo257580@kali: /root
Archivo Editar Ver Buscar Terminal Ayuda
uo257580@kali:/root$ sudo apt-get install tcpdump apparmor-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
tcpdump ya está en su versión más reciente (4.9.2-3).
fijado tcpdump como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
gdal-bin gdal-data libaec0 libarmadillo9 libarpac2
libboost-program-options1.62.0 libboost-serialization1.62.0
libboost-test1.62.0 libboost-timer1.62.0 libcgall3 libcharls1 libdap25
libdapclient6v5 libdapserver7v5 libdee-1.0-4 libepsilon1 libfcgi-bin
libfcgi0ldbl libfreeexl1 libfyba0 libgdal20 libgeotiff2 libgmime-3.0-0
libgtk2-perl libhdf4-0-alt libhdf5-100 libjemalloc1 libkmlbase1
libkmlconvenience1 libkmlcore1 libkmlengine1 libkmlregionator1 libkmlxsd1
liblwgeom-2.5-0 liblwgeom-dev libnetcdf13 libogdi3.2 libpango-perl
libpyside1.2 libqca2 libqca2-plugins libqgis-analysis2.18.24
libqgis-core2.18.24 libqgis-customwidgets libqgis-gui2.18.24
libqgis-networkanalysis2.18.24 libqgis-server2.18.24 libqgispython2.18.24
libqhull7 libqtwebkit4 libqt6abi1 libsane-extras libsane-extras-common
libsfcall1 libshiboken1.2v5 libspatialindex4v5 libspatialite7 libsuperlu5
libsz2 libunbound2 liburiparser1 libwhisker2-perl libxapian30 libxerces-c3.2
libzeitgeist-2.0-0 odbcinst odbcinst1debian2 php7.2-mysql
python-backports.functools-lru-cache python-backports.ssl-match-hostname

```

- Instalar swig

```

uo257580@kali: /root
Archivo Editar Ver Buscar Terminal Ayuda
uo257580@kali:/root$ sudo apt-get install swig
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
swig ya está en su versión más reciente (3.0.12-2).
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
gdal-bin gdal-data libaec0 libarmadillo9 libarpac2
libboost-program-options1.62.0 libboost-serialization1.62.0
libboost-test1.62.0 libboost-timer1.62.0 libcgall3 libcharls1 libdap25
libdapclient6v5 libdapserver7v5 libdee-1.0-4 libepsilon1 libfcgi-bin
libfcgi0ldbl libfreeexl1 libfyba0 libgdal20 libgeotiff2 libgmime-3.0-0
libgtk2-perl libhdf4-0-alt libhdf5-100 libjemalloc1 libkmlbase1
libkmlconvenience1 libkmlcore1 libkmlengine1 libkmlregionator1 libkmlxsd1
liblwgeom-2.5-0 liblwgeom-dev libnetcdf13 libogdi3.2 libpango-perl
libpyside1.2 libqca2 libqca2-plugins libqgis-analysis2.18.24
libqgis-core2.18.24 libqgis-customwidgets libqgis-gui2.18.24
libqgis-networkanalysis2.18.24 libqgis-server2.18.24 libqgispython2.18.24
libqhull7 libqtwebkit4 libqt6abi1 libsane-extras libsane-extras-common
libsfcall1 libshiboken1.2v5 libspatialindex4v5 libspatialite7 libsuperlu5
libsz2 libunbound2 liburiparser1 libwhisker2-perl libxapian30 libxerces-c3.2
libzeitgeist-2.0-0 odbcinst odbcinst1debian2 php7.2-mysql
python-backports.functools-lru-cache python-backports.ssl-match-hostname
python-cycler python-gdal python-kiwisolver python-matplotlib python-owslib

```

Ahora, ya podemos instalar Cuckoo. En este caso nos bajaremos Cuckoo desde el repositorio oficial:

```
uo257580@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
uo257580@kali:~$ sudo git clone https://github.com/cuckoosandbox/cuckoo.git  
Clonando en 'cuckoo'...  
remote: Enumerating objects: 61920, done.  
remote: Total 61920 (delta 0), reused 0 (delta 0), pack-reused 61920  
Recibiendo objetos: 100% (61920/61920), 48.93 MiB | 10.51 MiB/s, listo.  
Resolviendo deltas: 100% (40580/40580), listo.  
uo257580@kali:~$  
  
uo257580@kali: ~/cuckoo/stuff  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
uo257580@kali:~$ virtualenv /tmp/cuckoo-development/  
Running virtualenv with interpreter /usr/bin/python2  
New python executable in /tmp/cuckoo-development/bin/python2  
Not overwriting existing python script /tmp/cuckoo-development/bin/python (you must use /tmp/cuckoo-development/bin/python2)  
Installing setuptools, pkg_resources, pip, wheel...done.  
uo257580@kali:~$ . /tmp/cuckoo-development/bin/activate  
(cuckoo-development) uo257580@kali:~$ cd cuckoo/  
(cuckoo-development) uo257580@kali:~/cuckoo$ cd stuff/  
(cuckoo-development) uo257580@kali:~/cuckoo/stuff$ sudo mo  
moc          montage          mount.lowntfs-3g  
moc-qt4      montage-im6       mount.ntfs  
modinfo      montage-im6.q16  mount.ntfs-3g  
modprobe     more             mountpoint  
mogrify       mount            mousetweaks  
mogrify-im6   mount.exfat      movemail  
mogrify-im6.q16 mount.exfat-fuse movemail.mailutils  
monitor-sensor mount.fuse  
(cuckoo-development) uo257580@kali:~/cuckoo/stuff$ sudo python monitor.py  
[sudo] password for uo257580:  
  
uo257580@kali: ~/cuckoo  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
uo257580@kali:~/cuckoo$ sudo python stuff/monitor.py  
[sudo] password for uo257580:  
Fetching Cuckoo Community archive, this may take a little while.  
Extracting.. community-master/data/monitor/e071e63a66e831163a40abc45109fdf71fee8  
29e/inject-x64.exe  
Extracting.. community-master/data/monitor/e071e63a66e831163a40abc45109fdf71fee8  
29e/inject-x86.exe  
Extracting.. community-master/data/monitor/e071e63a66e831163a40abc45109fdf71fee8  
29e/is32bit.exe  
Extracting.. community-master/data/monitor/e071e63a66e831163a40abc45109fdf71fee8  
29e/monitor-x64.dll  
Extracting.. community-master/data/monitor/e071e63a66e831163a40abc45109fdf71fee8  
29e/monitor-x86.dll  
You're good to go now!  
uo257580@kali:~/cuckoo$
```



```
uo257580@kali: ~/cuckoo
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
uo257580@kali:~/cuckoo$ sudo python setup.py sdist develop
running sdist
running egg_info
creating Cuckoo.egg-info
writing requirements to Cuckoo.egg-info/requirements.txt
writing Cuckoo.egg-info/PKG-INFO
writing top-level names to Cuckoo.egg-info/top_level.txt
writing dependency links to Cuckoo.egg-info/dependency_links.txt
writing entry points to Cuckoo.egg-info/entry_points.txt
writing manifest file 'Cuckoo.egg-info/SOURCES.txt'
reading manifest file 'Cuckoo.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
warning: no previously-included files matching '*.pyc' found under directory '*'
warning: no previously-included files matching '*.pyo' found under directory '*'
warning: no previously-included files matching '*.map' found under directory '*'
writing manifest file 'Cuckoo.egg-info/SOURCES.txt'
running check
creating Cuckoo-2.0.7a1
creating Cuckoo-2.0.7a1/Cuckoo.egg-info
creating Cuckoo-2.0.7a1/cuckoo
creating Cuckoo-2.0.7a1/cuckoo/apps
creating Cuckoo-2.0.7a1/cuckoo/auxiliary
creating Cuckoo-2.0.7a1/cuckoo/common
creating Cuckoo-2.0.7a1/cuckoo/compat
```

A continuación, configuramos el directorio de trabajo

```
uo257580@kali: ~/cuckoo
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
uo257580@kali:~/cuckoo$ cuckoo -d
Most Visited
SSSS .S. SSSS .S. SSSS SSSS SSSS SSSS
d%%SP .SS SS. d%%SP .SS The first time d%%SP-YS%%b d%%SP-YS%%b will be
B d% do Work Directory S%S d%S' S%S S&S d%S' S%b d%S' S%b
S%S S%S S%S S%S S%S S&S S&S S&S S&S S&S
S&S S&S S&S S&S S&S S&S S&S S&S S&S
S&S S&S S&S S&S S&S S&S S&S S&S S&S
S&S S&S S&S S&S S&S S&S S&S S&S S&S
S*b Analysis S*b work Rout d+S S*b S*S S% S*b d+S S*b d+S
S*S. S*S. .S*S S*S. S*S S& S*S. .S*S S*S. .S*S
SSSbs SSSbs_sdSSS SSSbs S*S S& SSSbs_sdSSS SSSbs_sdSSS
YSSP YSSP-YSSY YSSP S*S SS YSSP-YSSY YSSP-YSSY
Preparing the Guest
Preparing the Guest (Physical Machine)
Cuckoo Sandbox 2.0.6
www.cuckoosandbox.org
Copyright (c) 2010-2018
=====
Welcome to Cuckoo Sandbox, this appears to be your first run!
We will now set you up with our default configuration.
```

```
uo257580@kali: ~/cuckoo
Archivo Editor Ver Buscar Terminal Ayuda
uo257580@kali:~/cuckoo$ sudo mkdir /opt/cuckoo
uo257580@kali:~/cuckoo$ sudo chown cuckoo:cuckoo /opt/cuckoo
uo257580@kali:~/cuckoo$ cuckoo --cwd /opt/cuckoo

Cuckoo Sandbox 2.0.6
www.cuckoosandbox.org
Copyright (c) 2010-2018

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, setup is now as
```

```
uo257580@kali: ~/cuckoo
GNU nano 3.2 /home/uo257580/.bashrc Modificado
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

export CUCKOO=/opt/cuckoo

# If not running interactively, don't do anything
case $- in
  *i*) ;;
  *) return;;
esac

Ver ayuda Guardar Buscar Cortar txt Justificar Posición
Salir Guardar Leer fich. Reemplazar Pegar txt Ortografía Ir a línea
```

```
uo257580@kali: ~/cuckoo
Archivo Editor Ver Buscar Terminal Ayuda
uo257580@kali:~/cuckoo$ cuckoo

Cuckoo Sandbox 2.0.6
www.cuckoosandbox.org
Copyright (c) 2010-2018
Cuckoo says there's a version
Checking for updates...
You're good to go!
Our latest blogposts:

In the case of VirtualBox the hostonly interface
vboxnet0 can be created as follows:

# If the hostonly interface vboxnet0 does not exist
$ sudo ifconfig vboxnet0 192.168.56.1 netmask 255.255.255.0
```

A PARTIR DE AQUÍ HE INSTALADO, HE BORRADO, HE AÑADIDO, HE VUELTO A INSTALAR Y A HACER MILES DE COSAS PERO NO ENTIENDO POR QUÉ MOTIVO ME SALTAN ERRORES POR TODOS LADOS, YA SEA CON LA INSTALACIÓN DE "MONGODB" QUE NO ME DEJA, Y LO HE INTENTADO DE MILES DE MANERAS, O INCLUSO CON OTRAS HERRAMIENTAS Y COMPONENTES NECESARIOS PARA EL DESPLIEGUE Y FUNCIONAMIENTO DE CUCKOO.

HASTA EL ÚLTIMO MOMENTO HE VISITADO DISTINTAS WEBS, HE VISTO DISTINTAS GUÍAS, HE REHECHO LO MISMO DE DISTINTAS MANERAS PERO NO HE DADO CON LA SOLUCIÓN, Y NO SE QUE REALMENTE HACER O POR QUÉ DEBE DE ESTAR FALLANDO TODO. HE SEGUIDO LA GUÍA DE LA PÁGINA OFICIAL DE CUCKOO PERO NO LO HE LOGRADO, ME HE APOLLADO EN OTRAS PÁGINAS WEBS, HE INTENTADO RESOLVER LOS ERRORES QUE ME DABA SOLICITANDO AYUDA A OTROS USUARIOS, O GRACIAS A SUS APORTACIONES, PERO NI AUN ASI HE CONSEGUIDO LO QUE QUERÍA.

ME FASTIDIA Y ME ENOJA LA SITUACIÓN YA QUE ES UNA HERRAMIENTA/PROGRAMA QUE ME PARECE MUY INTERESANTE Y ENTRETENIDA Y SOBRETUDO MUY ÚTIL (EN BASE A LOS VIDEOS QUE HE VISTO).

HE INTENADO INSTALAR CUCKOO DESDE LA PÁGINA WEB COMO ARCHIVO, POR OTROS MEDIOS, INCLUSO DESDE SU REPOSITORIO OFICIAL DE GITHUB PERO EL PROBLEMA HA SIDO TODOS LOS ERRORES QUE HE OBTENIDO A MEDIDA QUE HE IDO HACIENDO TODO, DE LO CUAL AL FINAL SOLAMENTE HE DEJADO CAPTURAS DEL PROCEDIMIENTO USANDO GITHUB, PERO TENIENDO UNAS 50 CAPTURAS DEL RESTO DE COSAS QUE HE HECHO, A PARTE.