ANALOG GROUP

Sprint 6

ENTORNO CONTROLADO CON CUCKOO

https://www.cuckoosandbox.org/

Grupo de Seguridad Informatica - UMSA

https://gsiumsa.fcpn.edu

GSI Grupo de Seguridad Informatica UMSA

1.-INSTALACION DE CUCKOO

la instalación de cuckoo no puede ser en una máquina virtual ya que cuckoo hace uso de virtualbox para manejar las máquinas virtuales.

Se recomienda la instalación de cuckoo en una distribución basada en debian o ubuntu.

todo como súper usuario, se recomienda usar la distribución **Backbox**:

```
$ add-apt-repository ppa:pi-rho/security
$ apt-get update
$ apt-get install volatility
$ apt-get install python python-pip python-dev libffi-dev libssl-dev python-virtualenv
pythonsetuptools libjpeg-dev zlib1g-dev swig  mongodb postgresql libpq-dev tcpdump apparmor-
utils swig
$ pip install -U pip setuptools
$ pip install -U cuckoo
$ groupadd pcap
$ usermod -a -G pcap <usuario>
$ chgrp pcap /usr/sbin/tcpdump
$ chmod 750 /usr/sbin/tcpdump
$ setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

- reiniciar el equipo
- abrir una terminal como usuario normal y escribir:

```
$ cuckoo
$ cuckoo -d
$ cuckoo comunity
```

IMPORTANTE

Esto generara la carpeta oculta ".cuckoo" en el directorio de usuario donde se encuentra los archivos de configuración, puede verse los archivos y carpetas ocultas presionando ctrl+h.

Carpeta oculta .cuckoo en el directorio de usuario bl455.

2.- INSTALANDO VIRTUALBOX:

```
wget -c http://download.virtualbox.org/virtualbox/5.1.22/virtualbox-5.1_5.1.22115126~Ubuntu~trusty_amd64.deb

wget -c http://download.virtualbox.org/virtualbox/5.1.22/Oracle_VM_VirtualBox_Extension_Pack5.1.22115126.vbox-extpack

sudo dpkg -i virtualbox-5.1_5.1.22-115126~Ubuntu~trusty_amd64.deb

instalar Oracle_VM_VirtualBox_Extension_Pack-5.1.22-115126.vbox-extpack haciendo 2 clicks
```

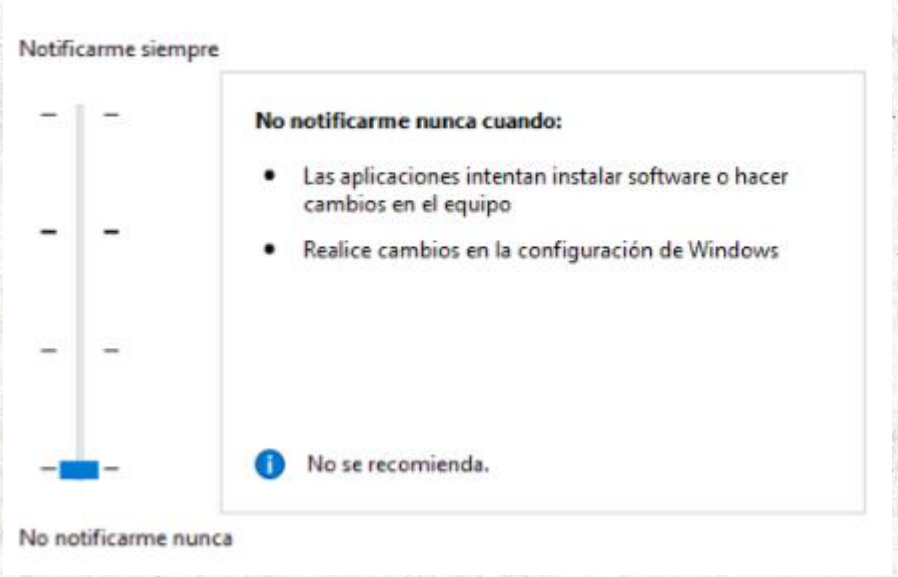
3.-PREPARACION DE MAQUINAS VIRTUALES

Se usarán las siguientes versiones de windows con sus respectivas versiones de office, su ip configurada manualmente en la maquina virtual y su modo de red en la configuración de virtualbox.

```
windows xp + office 2007,ip 192.168.56.101, modo de red "Host-Only adapter", interfaz "vboxnet0"
windows 7  + office 2010,ip 192.168.56.102, modo de red "Host-Only adapter", interfaz "vboxnet0"
windows 8  + office 2013,ip 192.168.56.103, modo de red "Host-Only adapter", interfaz "vboxnet0"
windows 10 + office 2016,ip 192.168.56.104, modo de red "Host-Only adapter", interfaz "vboxnet0"
```

Para todas las versiones:

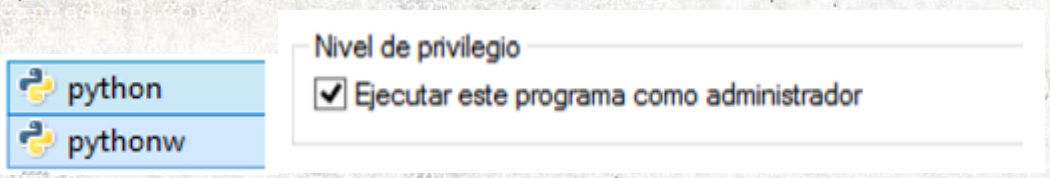
- windows y office deben estar activadas,
- **el firewall, las actualizaciones automáticas, el antivirus(Windows defender), el control de cuentas de usuario(UAC) deben estar desactivadas,**



UAC desactivado.

- el grupo de trabajo en todas debe ser la misma,
- la puerta de enlace para todas las maquinas es: 192.168.56.1
- instalar las "Guest additions"
- compartir una carpeta entre la máquina virtual y el equipo anfitrión(nosotros) esto para pasarle archivos a la máquina virtual
- instalar Python en cada equipo según su arquitectura

- los archivos “python” y “pythonw” ubicados en la carpeta de instalación de Python deben marcarse para ejecutarse como administrador



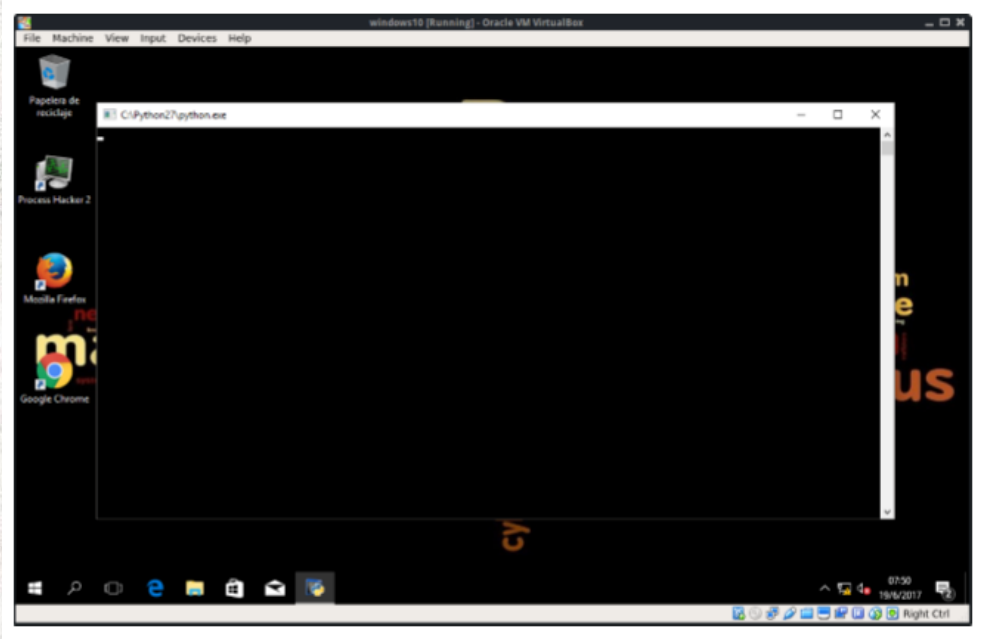
Los archivos deben ejecutarse como administrador.

- copiar el archivo "agent.py" ubicado en .cuckoo/agent a la unidad C: crear un archivo .bat con el siguiente contenido y copiar a la unidad C: y ejecutar en cada máquina virtual:

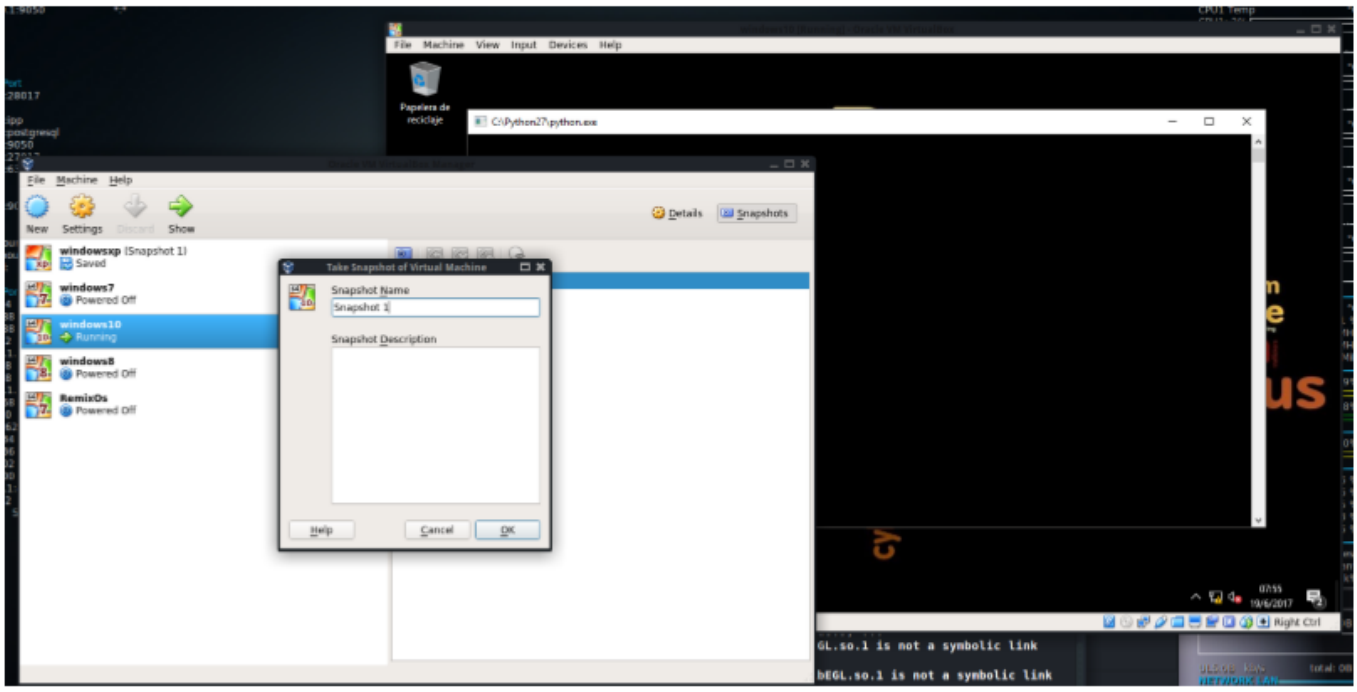
```
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /t Reg_Sz /v Agent /d
"C:agent.py"
pause
```

esto agrega al inicio el archivo "agent.py"

- hacer 2 click en el archivo agent.py, el escritorio de la máquina virtual debe quedar así con el “agent.py” en ejecución:



- crear un "Snapshot" de virtualbox para cada máquina una vez el archivo “agent.py” está en ejecución



Captura de un snapshot de nombre "Snpashot 1"

- Una vez tomado el snapshot podemos apagar la máquina virtual

Los Snapshot se utilizan para restaurar una máquina virtual a un estado anterior, cuckoo utiliza esta opción para recuperar una máquina virtual tras un análisis, imaginemos por un momento que el virus a analizar es altamente destructivo y la máquina virtual queda inutilizable entonces con esta opción cuckoo podrá restaurar la máquina virtual al estado en que se tomó el snapshot es por esta razón que se debe tomar un snapshot una vez se terminen de hacer las configuraciones así se tendrá un respaldo del estado inicial de una máquina virtual.

4.- CONFIGURACION CUCKOO

En la carpeta .cuckoo/conf se encuentran los archivos de configuración.

- entrar a la carpeta .cuckoo/conf
- editar el archivo cuckoo.conf y cambiar la línea:

machinery =
por
machinery = virtualbox

esto especifica el tipo de virtualizador que se usara

- editar el archivo virtualbox.conf y cambiar la línea:

machines =
por
machines =cuckoo1

cuckoo1 es el nombre de un perfil asociado a una versión de windows pueden haber mas perfiles,

- en la línea [cuckoo1] que indica ese perfil cambiar la línea:

label =
por
label = <nombre de la máquina virtual con windows>

en label se indica el nombre con el que se creo la máquina virtual en virtualbox ejemplo label = windowsxp

perfil de virtualbox con nombre "windowsxp"

- cambiar la línea:

platform =
por
platform = windows

- ip esta se cambia en función de la versión de windows que se usara

- en la línea snapshot debe estar el nombre del snapshot que le hicieron a la máquina virtual por defecto es "Snapshot 1" por lo tanto quedaría asi:

snapshot = Snapshot 1

El perfil "windowsxp" contiene un snapshot de nombre "Snapshot 1"

- Guarden cambios y cierren el archivo.

5.- EJECUTANDO CUCKOO

- En una terminal de usuario normal escribir:
  `$ cuckoo -d`

```
2017-06-18 00:04:01,881 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
[2017-06-18 00:04:03] Restoring virtual machine windowsxp to Snapshot 1
2017-06-18 00:04:03,601 [cuckoo.machinery.virtualbox] DEBUG: Restoring virtual machine windowsxp to Snapshot 1
[2017-06-18 00:04:04] Loaded 1 machine/s
2017-06-18 00:04:04,262 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
[2017-06-18 00:04:04] Waiting for analysis tasks.
2017-06-18 00:04:04,385 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
```

Ejecucion correcta de cuckoo a la espera de un análisis.

- en otra terminal escribir:

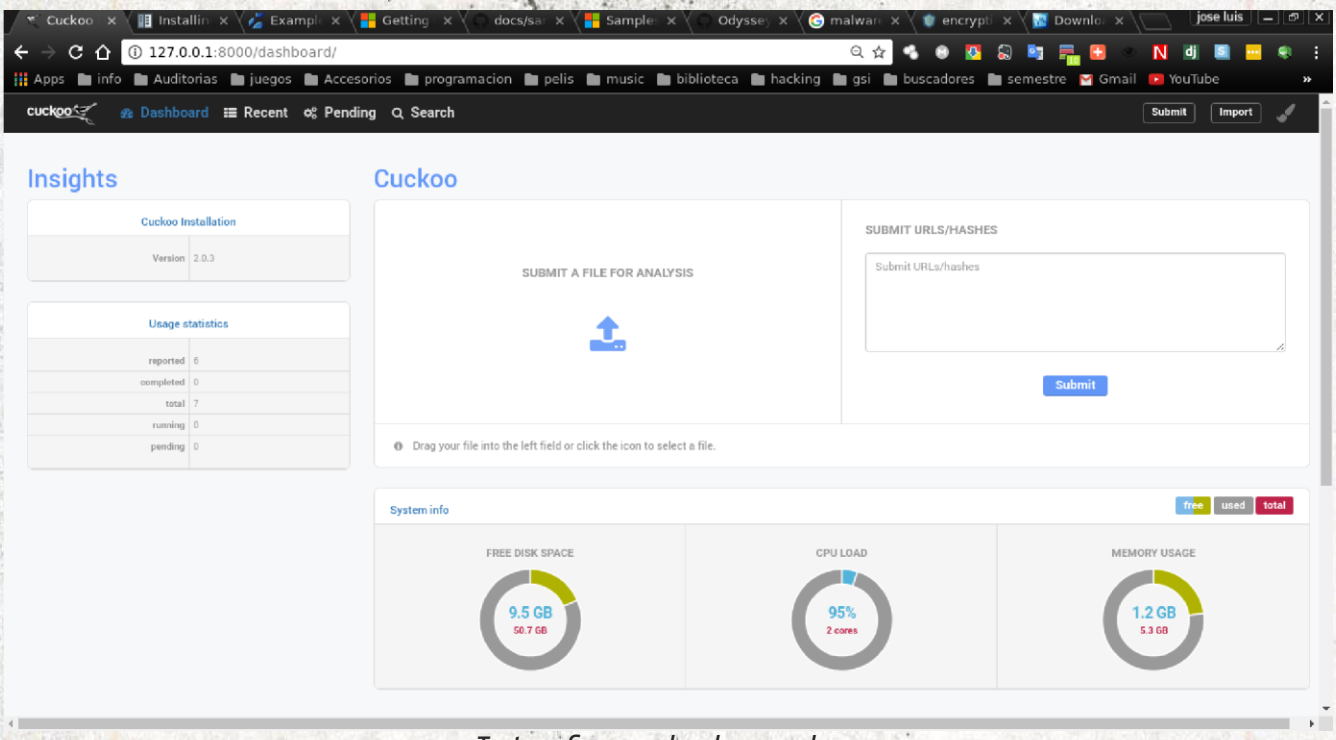
  `$ cuckoo web runserver`

```
$ cuckoo web runserver
[2017-06-18 00:05:11] No route found for IPv6 destination :: (no default route?)
[2017-06-18 00:05:27] No route found for IPv6 destination :: (no default route?)
Performing system checks...

System check identified no issues (0 silenced).
June 18, 2017 - 00:05:28
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

Cuckoo web server a la espera de conexiones

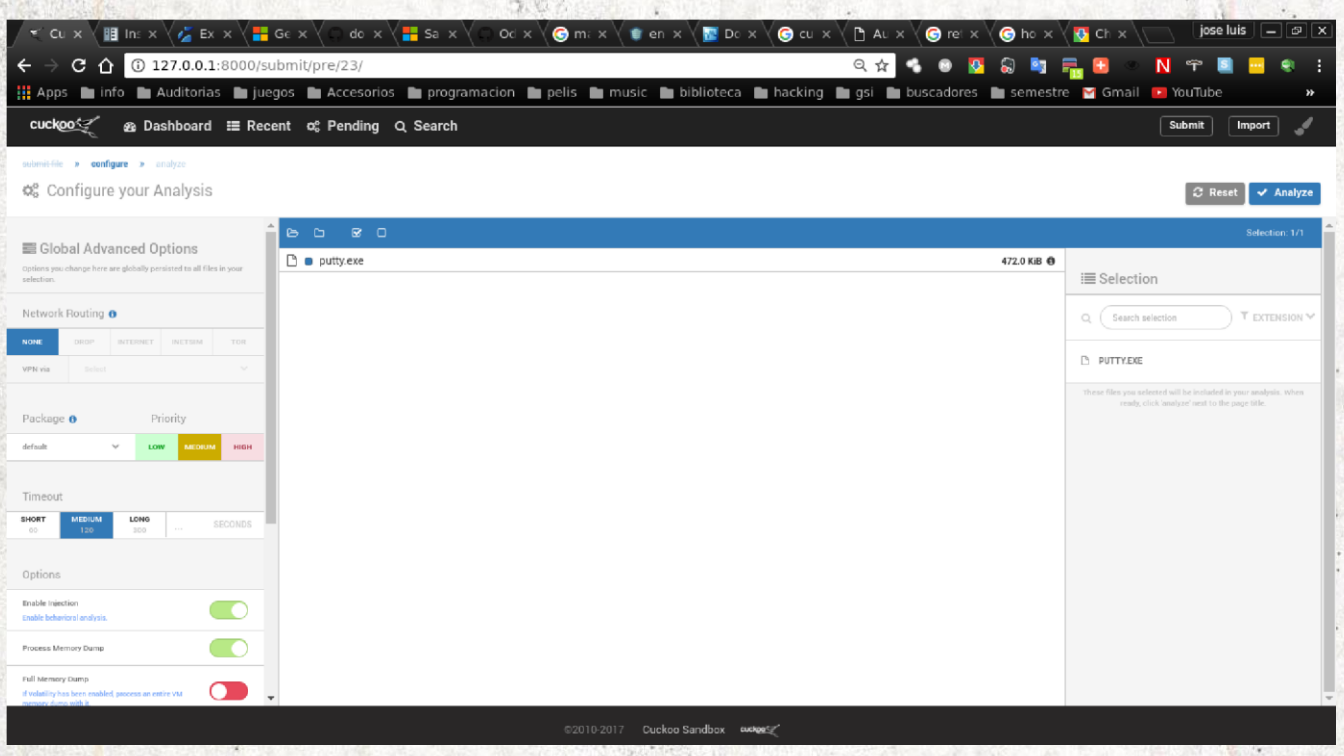
- esto habilitara la dirección 127.0.0.1:8000



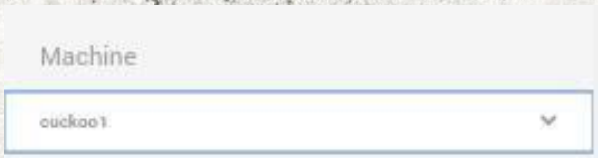
Interfaz web de cuckoo.

6- PRUEBA DE ANALISIS

Simplemente debe arrastrarse el archivo sospechoso hasta donde dice “SUBMIT A FILE FOR ANALISIS”, una vez subido el archivo veremos lo siguiente:



En la parte izquierda tenemos muchas opciones como elegir el tipo de extensión y la prioridad del análisis en esta misma sección al final podemos elegir el perfil asociado a cada versión de windows



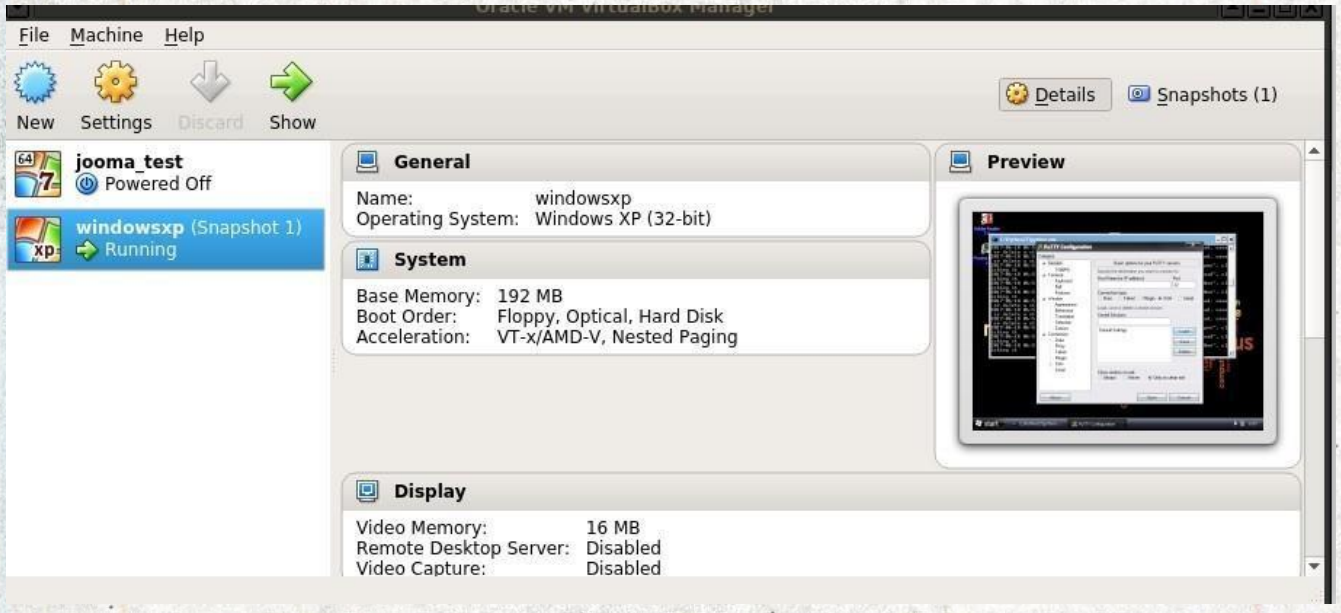
Selector de perfiles.

Cada opcion “cuckoo1” representa un perfil configurado en el archivo “virtualbox.conf” en nuestro caso una máquina virtual con windowsxp.

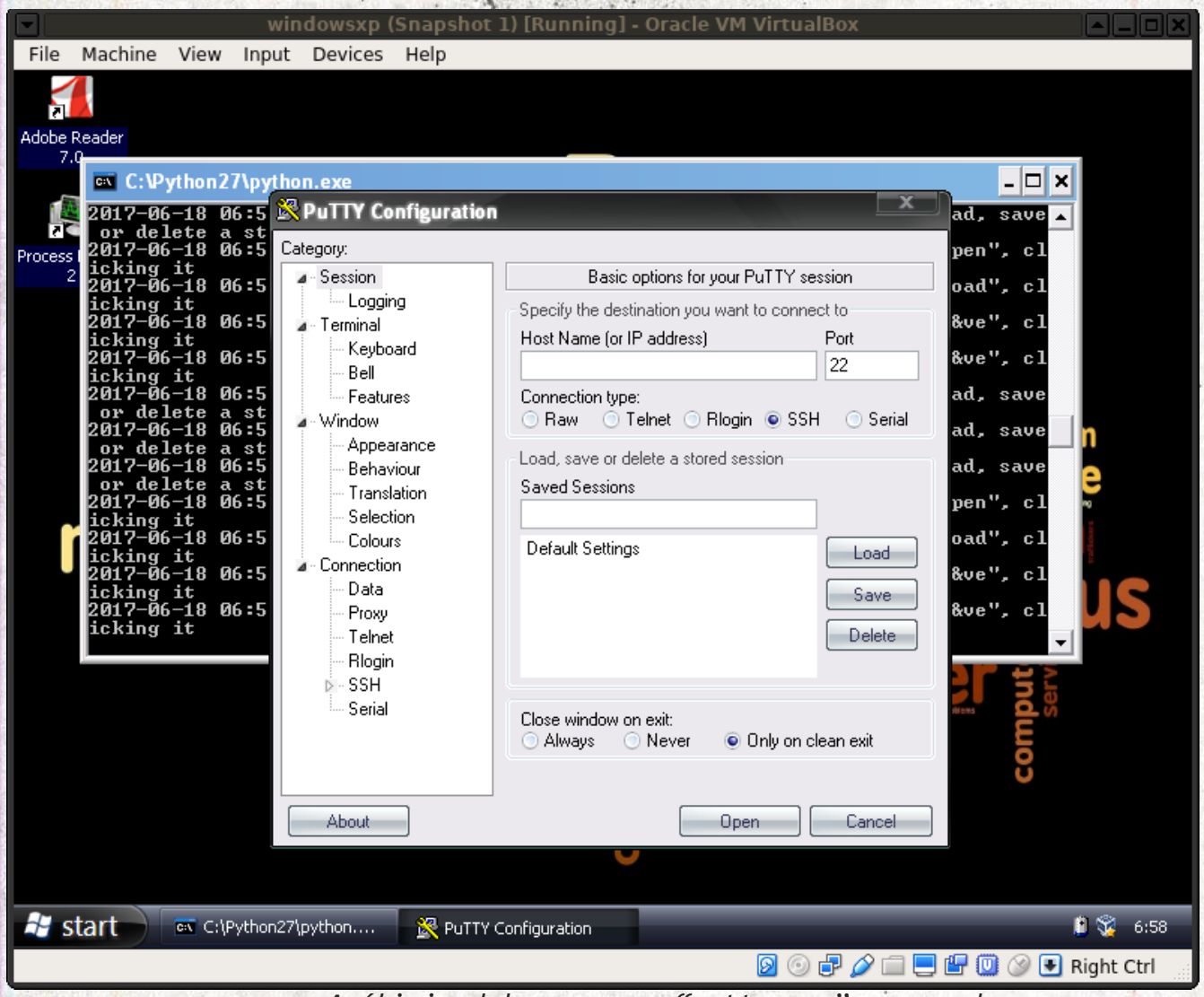
Ahora solo queda hacer el análisis

En la parte superior derecha hacemos click en “Analyze” para comenzar el análisis.

Mientras el análisis se ejecuta podemos ver lo que pasa en la máquina virtual claro solo “ver” ya que cualquier cambio que hagamos en la máquina virtual puede afectar los resultados solo debemos ir a virtualbox seleccionar nuestra maquina virtual y hacer click en “Show”



Virtualbox en ejecución de windowsxp.



Análisis del programa "putty.exe" con cuckoo.

La ejecución termina automáticamente y no necesita interacción con el usuario, una vez terminado el análisis este se verá en la interfaz web de cuckoo.

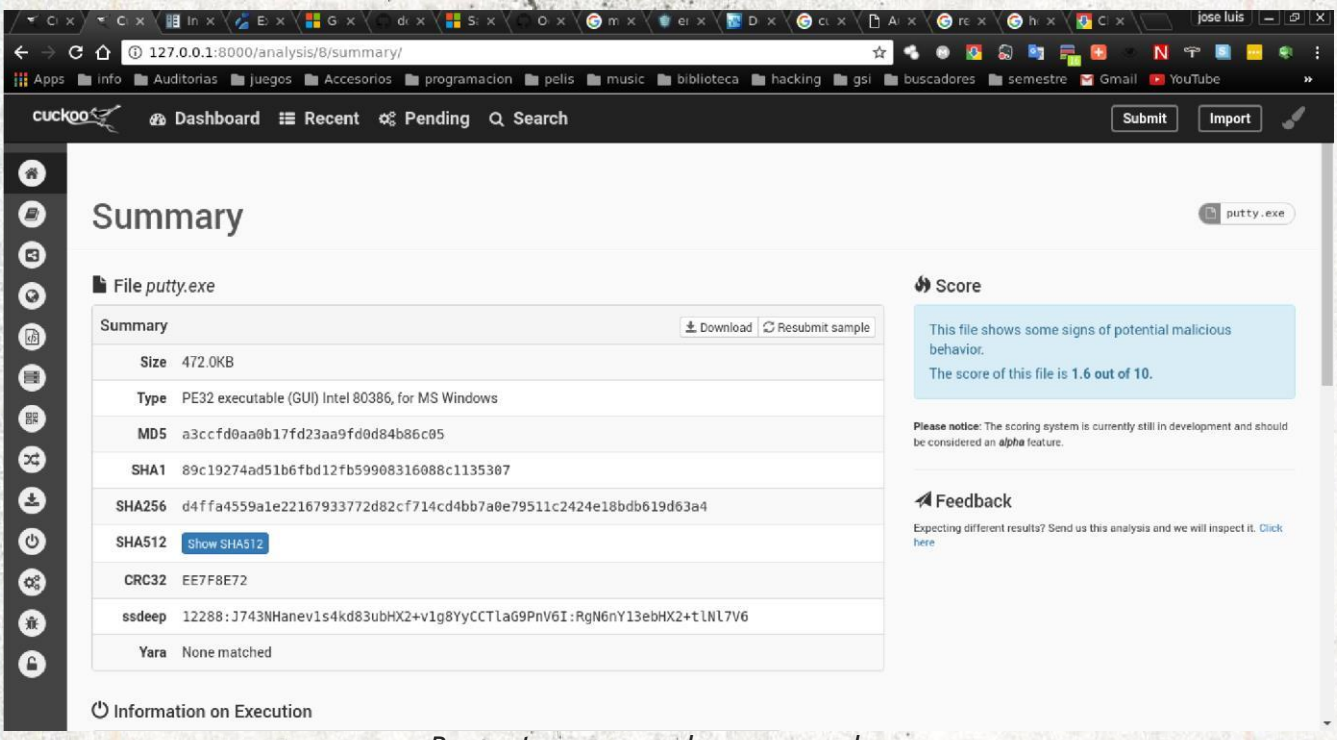
Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	Status
8	18/06/2017 00:56	putty.exe	exe	reported

Done

En "status" nos dice "reported" lo cual indica el fin del análisis.

Simplemente se hace click en toda la fila y este nos lleva al ver el reporte generado por cuckoo.



Reporte generado por cuckoo.

En el reporte podemos ver con gran detalle todo el análisis realizado por cucko desde los archivos generados y usados hasta las entradas del registro e intentos de conexiones al exterior todo esto es visible desde el lado izquierdo del reporte en los círculos.

7.- OPCIONES ONLINE DE CUCKOO

malwr

https://malwr.com/

Malwr es una muy buena opción para hacer pruebas al instante ofrece solo los resultados más relevantes como registros, procesos y conexiones, el único punto débil es que su análisis solo se basa en una versión de Windows XP y no en las más recientes pero aun así no deja de ser una muy buena opción.

linux.huntingmalware.com

Es la versión de cuckoo que se acaba de instalar pero únicamente para linux ofrece los mismos resultados pero solo admite archivos del tipo ELF, bash y python, lo más interesante es que puede hacer análisis en diferentes tipos de arquitectura desde arm hasta sparc.