

How to Download and Install

For all the command line instruction, they are all in red.

The credential for cuckoo user on this server is “`cuckoo:gatech6727`”

Follow these two videos and blogs

- https://www.youtube.com/watch?v=QIQS4gk_IFU
- <https://www.youtube.com/watch?v=FsF56772ZvU>
- <https://hatching.io/blog/cuckoo-sandbox-setup/>

Use python 2.7 to install because python 3 is not supported.

Create Virtual Environment

Change to cuckoo user and create a virtual environment. By activating the virtual environment, the packages installed by cuckoo is not going to affect the whole system.

```
sudo su cuckoo
virtualenv ~/cuckoo
. ~/cuckoo/bin/activate
```

All dependency packages are mentioned in the links above, including Windows ISO file, VirtualBox, and VMCloak.

For MongoDB, follow this link to install

- <https://www.cloudbooklet.com/how-to-install-mongodb-on-ubuntu-22-04/>

To install Distorm3, run `python2 -m pip install distorm3==3.4.2``

Create VM (automatically)

This information can also be found in the blog <https://hatching.io/blog/cuckoo-sandbox-setup/>

Setup Windows VM, it will use the ISO mounted earlier. The path it will try is /mnt/win7 and /mnt/win7x64 for win7

For this command, it initializes a x86-64 Windows 7 VM with 2 CPUs and 2048 MB RAM
`vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048`

Clone

This step is optional.

Clone the VM win7x64base into win7x64cuckoo, so that whatever changed to win7x64cuckoo won't affect win7x64base.

```
vmcloak clone win7x64base win7x64cuckoo
```

Snapshots

Create 4 snapshots, the IP address of the VM starts from 192.168.56.101 (101~104)

```
vmcloak snapshot --count 4 win7x64cuckoo 192.168.56.101
```

When creating snapshots, we may get errors “VBoxManage: error: Cannot change type for medium '/home/cuckoo/.vmcloak/image/win7x64cuckoo.vdi': the media type 'MultiAttach' can only be used on media registered with a machine that was created with VirtualBox 4.0 or later”

Use Chapter 6.1 from https://t0xicity.com/blog/cuckoo_sandbox/ to solve this issue.

List VMs

It shows up all the VMs that have already been created.

```
vmcloak list vms
```

How to Configure

Initialize

```
cuckoo init
```

The working directory will be “\$USERHOME/.cuckoo”, set up automatically.

Update Cuckoo Signatures

```
cuckoo community
```

Specify VirtualBox to GUI mode (optional, it will not show up if you're using X11)

```
$USERHOME/.cuckoo/conf/virtualbox.conf  
mode = gui
```

```
[virtualbox]  
# Specify which VirtualBox mode you want to run your machines on.  
# Can be "gui" or "headless". Please refer to VirtualBox's official  
# documentation to understand the differences.  
mode = headless
```

Add VMs to VirtualBox

It will read all the VMs using vmcloak add their information into configurations.

```
while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(vmcloak list vms)
```

The result will show in “\$USERHOME/.cuckoo/conf/virtualbox.conf”

Network Configuration

```
sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1  
sudo sysctl -w net.ipv4.conf.eth0.forwarding=1 (eth0 should be replace with your internet  
interface, you can find that with ifconfig. eno1 in my case)
```

Routing Configuration and Start Cuckoo

Run rooter at 1st panel

`cuckoo rooter --sudo --group cuckoo`

Then modify routing Internet in “\$USERHOME/.cuckoo/conf/virtualbox.conf.”

internet = <your internet interface>

```
[routing]
# Default network routing mode if none is specified by the user.
# In none mode we don't do any special routing - the VM doesn't have any
# network access (this has been the default actually for quite a while) aside
# from the subnet it exists in.
# In internet mode by default all the VMs will be routed through the network
# interface configured below (the "dirty line").
# And in VPN mode by default the VMs will be routed through the VPN identified
# by the given name of the VPN (as per the VPNs listed in the vpn section).
# Note that just like enabling VPN configuration setting this option to
# anything other than "none" requires one to run utils/rooter.py as root next
# to the Cuckoo instance (as it's required for setting up the routing).
route = none

# Network interface that allows a VM to connect to the entire internet, the
# "dirty line" so to say. Note that, just like with the VPNs, this will allow
# malicious traffic through your network. So think twice before enabling it.
# (For example, to use eth0 as dirty line: "internet = eth0").
internet = eno1
```

In the 2nd panel, run “cuckoo”

And in the 3rd panel, run “cuckoo web --host 127.0.0.1 --port 8080” to start the web interface.

<pre>2022-09-07 18:48:40,023 [cuckoo.apps.rooter] INFO: Processi ng command: state_disable 2022-09-07 18:48:40,030 [cuckoo.apps.rooter] INFO: Processi ng command: state_enable 2022-09-07 18:48:40,073 [cuckoo.apps.rooter] INFO: Processi ng command: nic_available eno1 2022-09-07 18:48:40,078 [cuckoo.apps.rooter] INFO: Processi ng command: rt_available main 2022-09-07 18:48:40,081 [cuckoo.apps.rooter] INFO: Processi ng command: disable_nat eno1 2022-09-07 18:48:40,090 [cuckoo.apps.rooter] INFO: Processi ng command: enable_nat eno1 2022-09-07 18:48:40,121 [cuckoo.apps.rooter] INFO: Processi ng command: flush_rtttable main 2022-09-07 18:48:40,121 [cuckoo.apps.rooter] INFO: Processi ng command: init_rtttable main eno1</pre>	<pre>* Cuckoo Sandbox 2.0.6, June 07, 2018. Interim release awaiting the big release. More at https://cuckoosandbox.org/blog/206-interim-relea se 2022-09-07 18:48:27, [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager 2022-09-07 18:48:28,199 [cuckoo.core.scheduler] INFO: Load ed 4 machine/s 2022-09-07 18:48:28,202 [cuckoo.core.scheduler] WARNING: As you've configured Cuckoo to execute parallel analyses, we recommend you to switch to a MySQL or a PostgreSQL database as SQLite might cause some issues. 2022-09-07 18:48:28,237 [cuckoo.core.scheduler] INFO: Waiti ng for analysis tasks.</pre>
<pre>/home/cuckoo/.local/lib/python2.7/site-packages/sflock/deco de/office.py:12: CryptographyDeprecationWarning: Python 2 i s no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed i n the next release. from cryptography.hazmat.backends import default_backend Performing system checks... System check identified no issues (0 silenced). September 07, 2022 - 18:48:40 Django version 1.8.4, using settings 'cuckoo.web.web.settin gs' Starting development server at http://127.0.0.1:8080/ Quit the server with CONTROL-C.</pre>	<pre>from cryptography.hazmat.backends import default_backend Success: File "/home/cuckoo/ransomwaRE.exe" added as task w ith ID #1 (cuckoo) cuckoo@bird:~\$ cuckoo submit malware-dyn-vs19-vari ant0.exe /home/cuckoo/.local/lib/python2.7/site-packages/sflock/deco de/office.py:12: CryptographyDeprecationWarning: Python 2 i s no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed i n the next release. from cryptography.hazmat.backends import default_backend Success: File "/home/cuckoo/malware-dyn-vs19-variant0.exe" added as task with ID #2 (cuckoo) cuckoo@bird:~\$ cuckoo submit malware-dyn-vs19-vari ant0.exe</pre>

[0] 0:~\$ "bird.gtisc.gatech.edu" 18:48 07-Sep-22

Forward the port with ssh to localhost if you're using X11. Run this command from your host laptop.

```
ssh -L 8080:localhost:8080 twang626@143.215.130.251
```

And we can access web interface from your laptop at <http://localhost:8080/>

To submit a sample to cuckoo sandbox, run

```
cuckoo submit <file>
```

Report

```
~/cuckoo/storage/analyses/<id>/reports/report.json
```

To get behavioral analysis

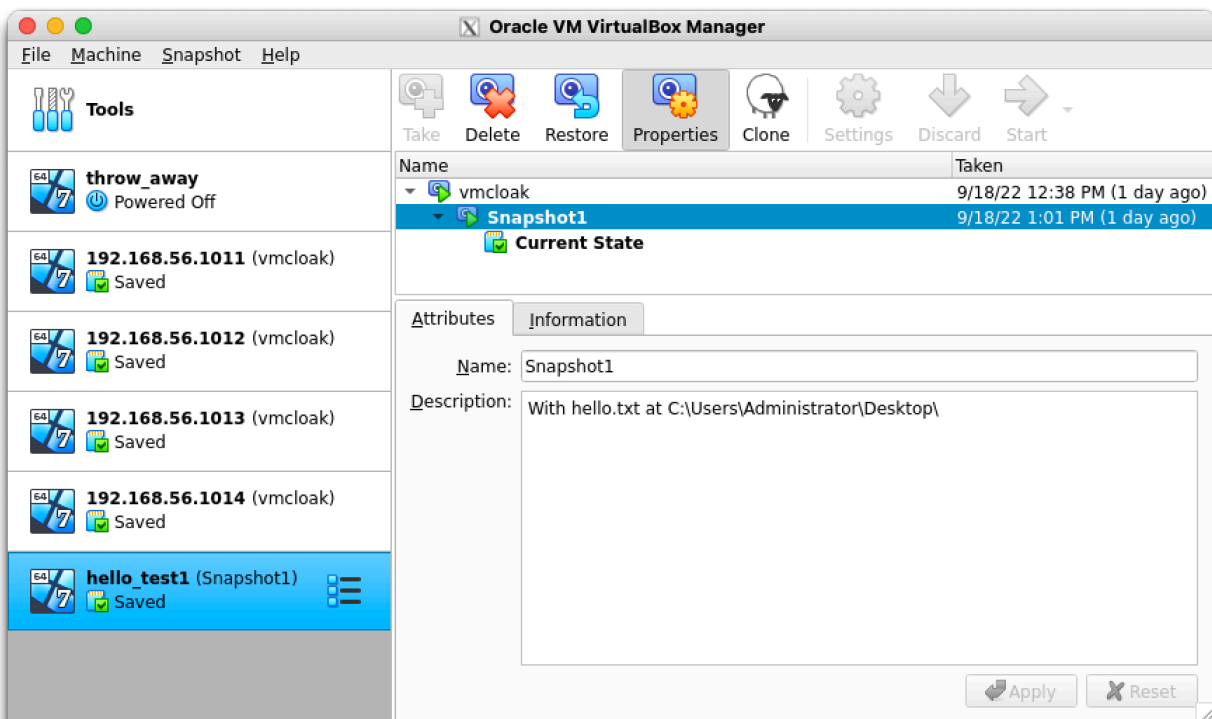
```
cat storage/analyses/<id>/reports/report.json | jq '.behavior'
```

To get screenshots

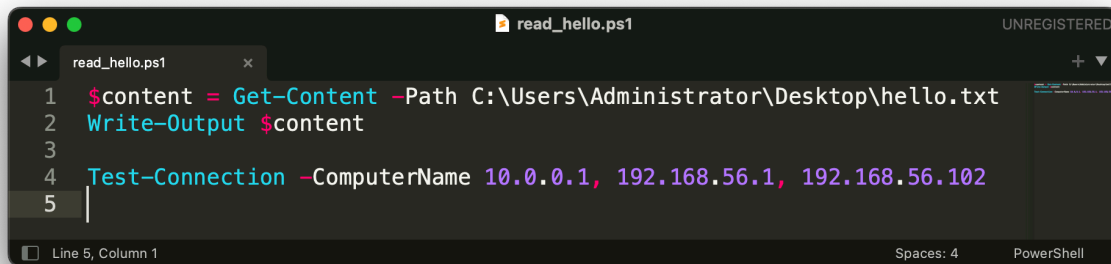
```
ls ~/cuckoo/storage/analyses/<id>/shots/
```

Test connectivity and file readability

First, put a file hello.txt into the virtual machine, and create a snapshot.



Then, create a script that reads hello.txt and test network connectivity.



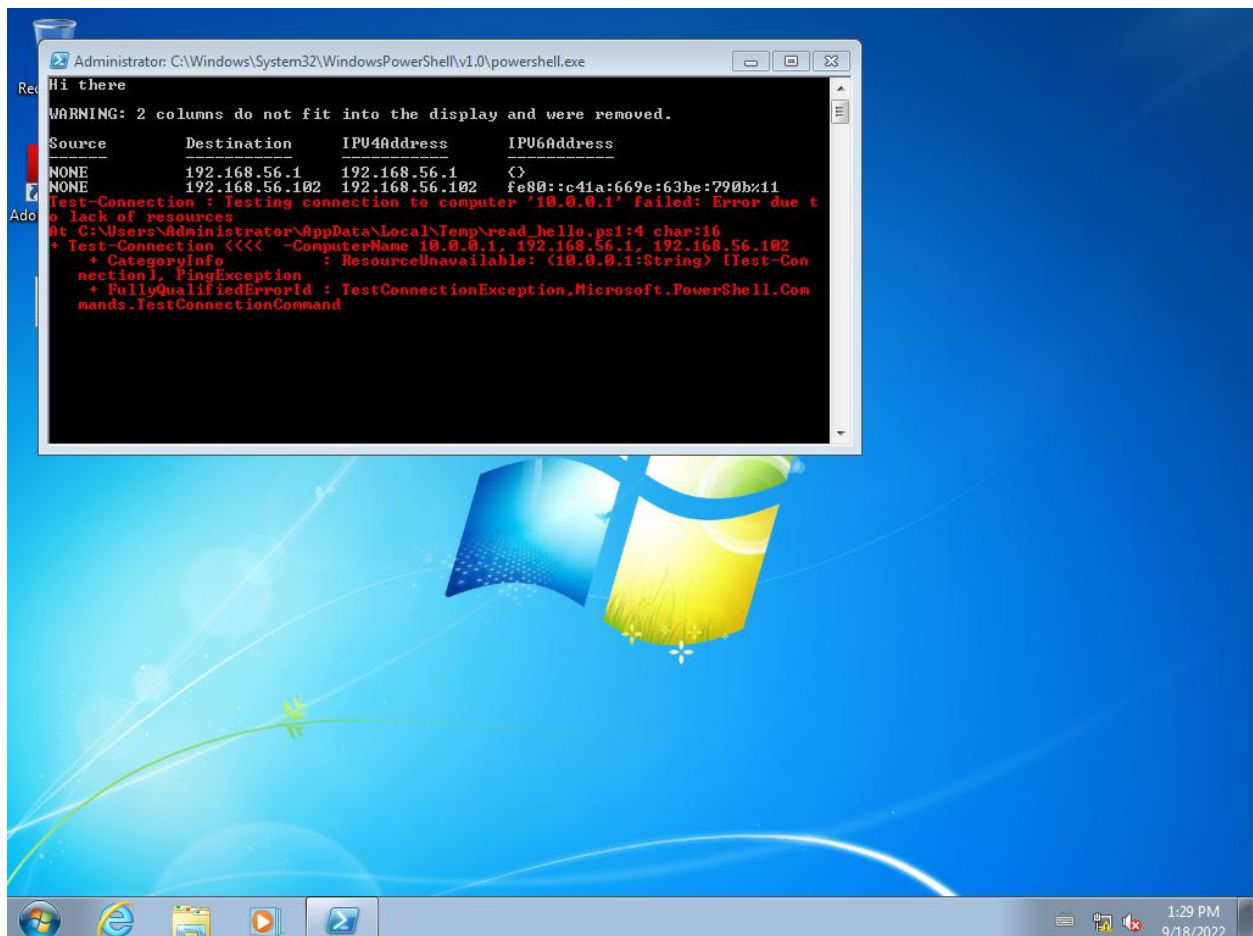
```
1 $content = Get-Content -Path C:\Users\Administrator\Desktop\hello.txt
2 Write-Output $content
3
4 Test-Connection -ComputerName 10.0.0.1, 192.168.56.1, 192.168.56.102
5
```

To test the network connectivity of one VM to another, we have to power on another VM. In my case, it's 192.168.56.102.

Finally, submit the script to our targeted VM in Cuckoo Sandbox.

`cuckoo submit read_hello.ps1 --machine hello_test1`

Here's the result, "Hi there" is the content of hello.txt that has already been put into VM earlier. 192.168.56.1 is the host machine IP address, and 192.168.56.102 is another VM address. 10.0.0.1 is a random address I used to showcase how it looks if an address is not reachable.



In conclusion, samples submitted to Cuckoo sandbox has the ability to read files in VM and connect to other VMs.