Cuckoo modified

Information Security Inc.

Contents

- About Cuckoo?
- About Cuckoo modified
- Cuckoo Testing Environment
- Cuckoo modified Installation (guest OS)
- Cuckoo modified Installation
- Submit a file through the web interface
- References

About Cuckoo

- Cuckoo is an open source automated malware analysis system.
- It's used to automatically run and analyze files and collect comprehensive analysis results that outline what the malware does while running inside an isolated Windows operating system

About Cuckoo modified

- Cuckoo modified is a forked, modified version of Cuckoo (https://github.com/spender-sandbox/cuckoo-modified)

- Advantages over the original Cuckoo

A) Fully-normalized file and registry names
B) 64-bit analysis
C) Handling of WoW64 filesystem redirection
D) Many additional API hooks
E) Service monitoring
F) Correlates API calls to malware call chains
G) Ability to follow APC injection and stealth explorer injection
H) Pretty-printed API flags
I) Per-analysis Tor support
J) Over 150 new signature modules (over 75 developed solely by Optiv)
K) Anti-anti-sandbox and anti-anti-VM techniques built-in
L) More stable hooking
M) Ability to restore removed hooks
N) Greatly improved behavioral analysis and signature module API
O) Ability to post comments about analyses
P) Deep hooks in IE's JavaScript and DOM engines usable for Exploit Kit identification
Q) Automatic extraction and submission of interesting files from ZIPs, RARs, RFC 2822 emails (.eml), and Outlook .msg files
R) Direct submission of AV quarantine files (Forefront, McAfee, Trend Micro, Kaspersky, MalwareBytes, MSE/SCEP, and SEP12 formats currently supported)
S) Automatic malware classification by Malheur

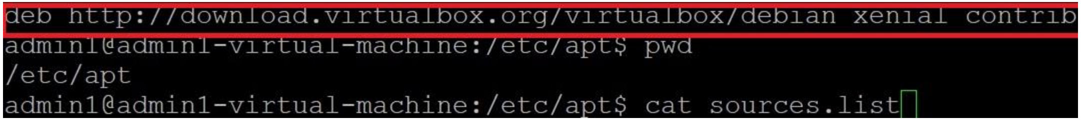
Cuckoo Testing Environment

- Host machine: Ubuntu Desktop 16.04.3 LTS
- Virtual environment: VirtualBox

Cuckoo modified Installation (guest OS)

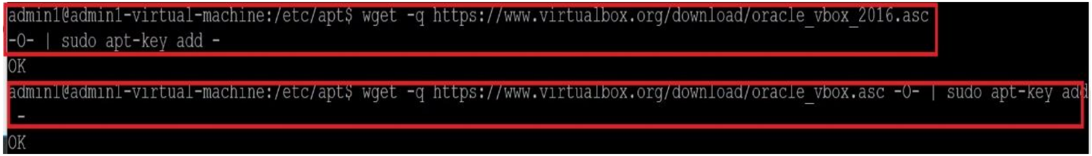
- Install VirtualBox

◎ Setup apt repository



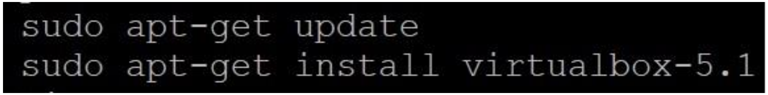
```
deb http://download.virtualbox.org/virtualbox/debian xenial contrib
admin1@admin1-virtual-machine:/etc/apt$ pwd
/etc/apt
admin1@admin1-virtual-machine:/etc/apt$ cat sources.list
```

◎ Setup Oracle public key



```
admin1@admin1-virtual-machine:/etc/apt$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc
-O- | sudo apt-key add -
OK
admin1@admin1-virtual-machine:/etc/apt$ wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add
 -
OK
```

◎ Install Oracle VirtualBox

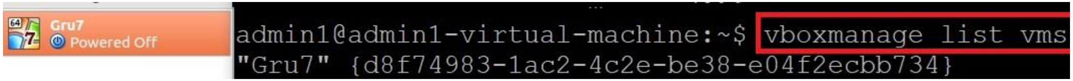


```
 sudo apt-get update
 sudo apt-get install virtualbox-5.1
```

Cuckoo modified Installation (guest OS)

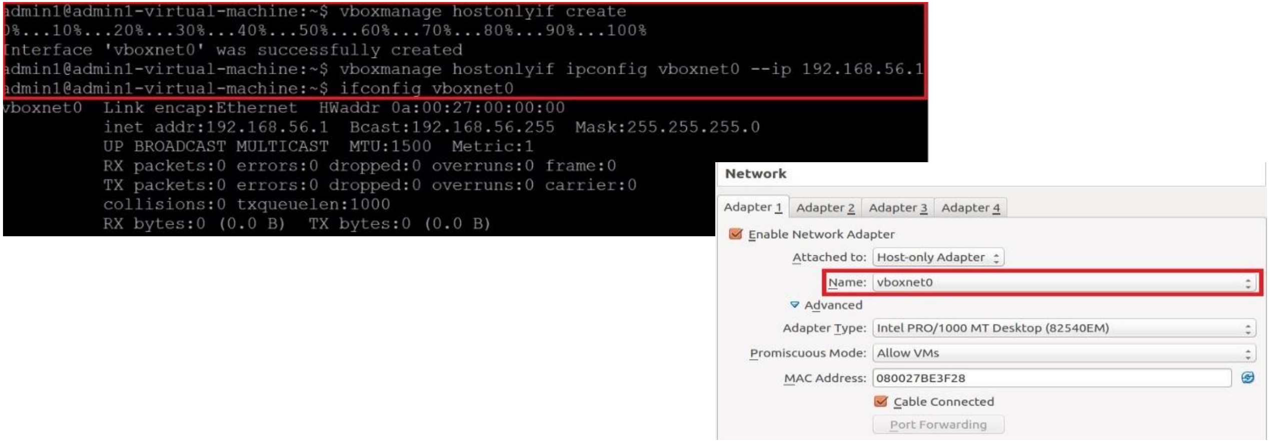
- Create and Configure Guest VM (VirtualBox)

◎ Install Guest OS (Windows 7 x64)



```
admin1@admin1-virtual-machine:~$ vboxmanage list vms
"Gru7" {d8f74983-1ac2-4c2e-be38-e04f2ecbb734}
```

◎ Configure host-only network



```
admin1@admin1-virtual-machine:~$ vboxmanage hostonlyif create
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interface 'vboxnet0' was successfully created
admin1@admin1-virtual-machine:~$ vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
admin1@admin1-virtual-machine:~$ ifconfig vboxnet0
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
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet0

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow VMs

MAC Address: 080027BE3F28

☑ Cable Connected

Cuckoo modified Installation (guest OS)

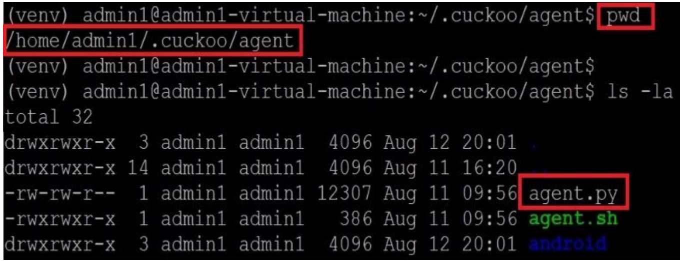
- To make Cuckoo run properly in the virtualized Windows system, install some required software and libraries

◎ Install Python (https://www.python.org/ftp/python/2.7.13/python-2.7.13.msi)

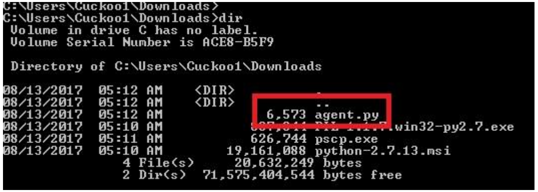
◎ Install Python Image libray (http://www.pythonware.com/products/pil/)

◎ Turn off windows firewall, automatic updates and disable UAC

◎ Install the agent

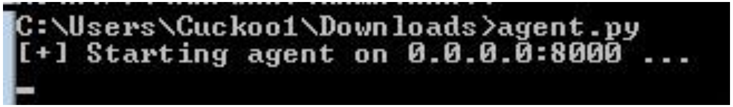


```
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ pwd
/home/admin1/.cuckoo/agent
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$
(venv) admin1@admin1-virtual-machine:~/.cuckoo/agent$ ls -la
total 32
drwxrwxr-x  3 admin1 admin1  4096 Aug 12 20:01 .
drwxrwxr-x 14 admin1 admin1  4096 Aug 11 16:20 ..
-rw-rw-r--  1 admin1 admin1 12307 Aug 11 09:56 agent.py
-rwxrwxr-x  1 admin1 admin1   386 Aug 11 09:56 agent.sh
drwxrwxr-x  3 admin1 admin1  4096 Aug 12 20:01 android
```



```
C:\Users\Cuckoo1\Downloads>
C:\Users\Cuckoo1\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is ACE8-B5F9

 Directory of C:\Users\Cuckoo1\Downloads

08/13/2017  05:12 AM    <DIR>          .
08/13/2017  05:12 AM    <DIR>          ..
08/13/2017  05:12 AM             6,573 agent.py
08/13/2017  05:10 AM     [illegible] PIL-1.1.7.win32-py2.7.exe
08/13/2017  05:11 AM           626,744 pscp.exe
08/13/2017  05:10 AM        19,161,088 python-2.7.13.msi
               4 File(s)     20,632,249 bytes
               2 Dir(s)  71,575,404,544 bytes free
```

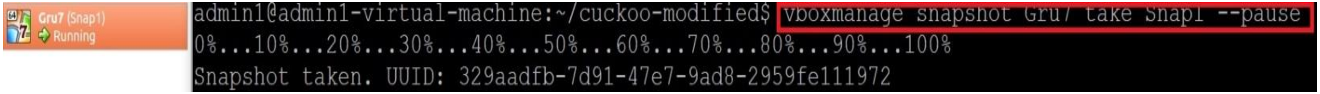
◎ Run the Agent



```
C:\Users\Cuckoo1\Downloads>agent.py
[+] Starting agent on 0.0.0.0:8000 ...
_
```

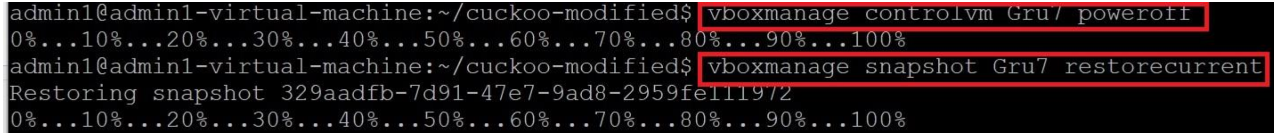
Cuckoo modified Installation (guest OS)

◎ Saving the virtual machine



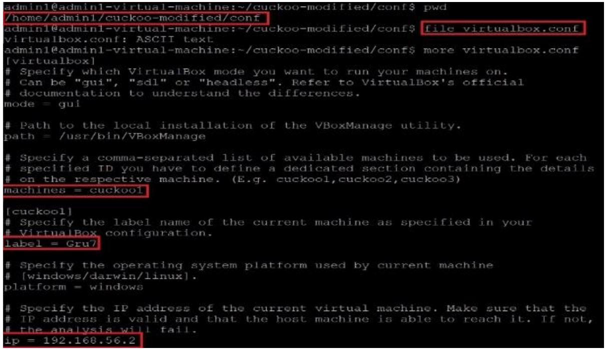
```
admin1@admin1-virtual-machine:~/cuckoo-modified$ vboxmanage snapshot Gru7 take Snap1 --pause
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Snapshot taken. UUID: 329aadfb-7d91-47e7-9ad8-2959fe111972
```

◎ Power off the machine and restore it



```
admin1@admin1-virtual-machine:~/cuckoo-modified$ vboxmanage controlvm Gru7 poweroff
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
admin1@admin1-virtual-machine:~/cuckoo-modified$ vboxmanage snapshot Gru7 restorecurrent
Restoring snapshot 329aadfb-7d91-47e7-9ad8-2959fe111972
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

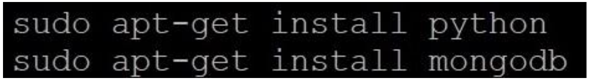
◎ Edit virtualbox.conf



```
admin1@admin1-virtual-machine:~/cuckoo-modified/conf$ pwd
/home/admin1/cuckoo-modified/conf
admin1@admin1-virtual-machine:~/cuckoo-modified/conf$ file virtualbox.conf
virtualbox.conf: ASCII text
admin1@admin1-virtual-machine:~/cuckoo-modified/conf$ more virtualbox.conf
[virtualbox]
# Specify which VirtualBox mode you want to run your machines on.
# Can be "gui", "sdl" or "headless". Refer to VirtualBox's official
# documentation to understand the differences.
mode = gui

# Path to the local installation of the VBoxManage utility.
path = /usr/bin/VBoxManage

# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1

[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = Gru7

# Specify the operating system platform used by current machine
# [windows/darwin/linux].
platform = windows

# Specify the IP address of the current virtual machine. Make sure that the
# IP address is valid and that the host machine is able to reach it. If not,
# the analysis will fail.
ip = 192.168.56.2
```

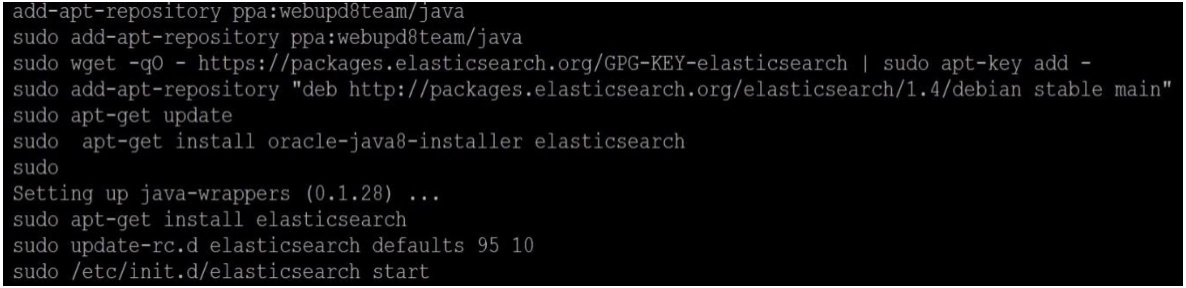
Cuckoo modified Installation

- Install Python, MongoDB (to use Django-based web interface)



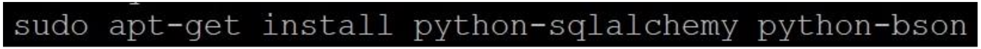
```
sudo apt-get install python
sudo apt-get install mongodb
```

- Install ElasticSearch



```
add-apt-repository ppa:webupd8team/java
sudo add-apt-repository ppa:webupd8team/java
sudo wget -qO - https://packages.elasticsearch.org/GPG-KEY-elasticsearch | sudo apt-key add -
sudo add-apt-repository "deb http://packages.elasticsearch.org/elasticsearch/1.4/debian stable main"
sudo apt-get update
sudo  apt-get install oracle-java8-installer elasticsearch
sudo
Setting up java-wrappers (0.1.28) ...
sudo apt-get install elasticsearch
sudo update-rc.d elasticsearch defaults 95 10
sudo /etc/init.d/elasticsearch start
```

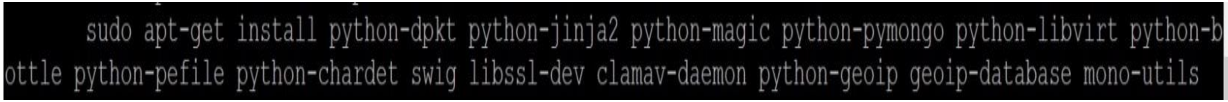
- Install SQLAlchemy and Python BSOn



```
sudo apt-get install python-sqlalchemy python-bson
```

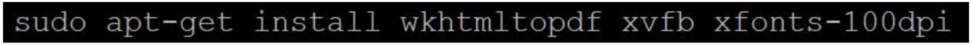
Cuckoo modified Installation

- Install optional dependencies



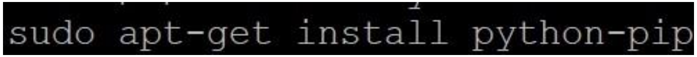
```
      sudo apt-get install python-dpkt python-jinja2 python-magic python-pymongo python-libvirt python-b
ottle python-pefile python-chardet swig libssl-dev clamav-daemon python-geoip geoip-database mono-utils
```

- For faster generation of PDF reports install wkhtmltopdf



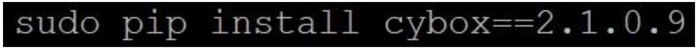
```
sudo apt-get install wkhtmltopdf xvfb xfonts-100dpi
```

- If Pip is not installed, install Pip

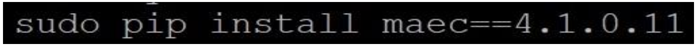


```
sudo apt-get install python-pip
```

- Install Cybox and Maec



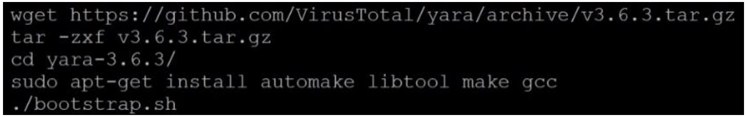
```
sudo pip install cybox==2.1.0.9
```



```
sudo pip install maec==4.1.0.11
```

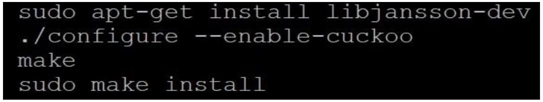
Cuckoo modified Installation

- Install YARA



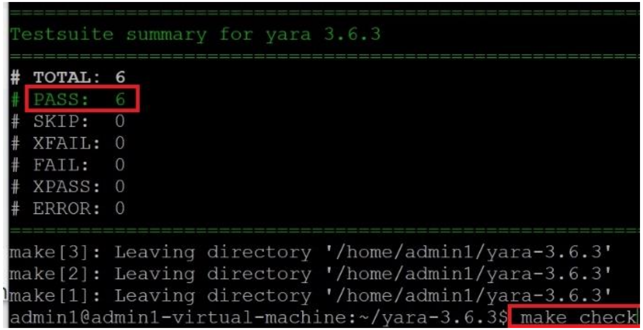
```
wget https://github.com/VirusTotal/yara/archive/v3.6.3.tar.gz
tar -zxf v3.6.3.tar.gz
cd yara-3.6.3/
sudo apt-get install automake libtool make gcc
./bootstrap.sh
```

- Compile YARA with Cuckoo module



```
sudo apt-get install libjansson-dev
./configure --enable-cuckoo
make
sudo make install
```

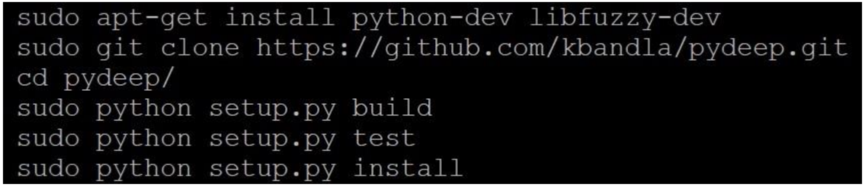
- Run the test cases to make sure everything is fine



```
============================================================================
Testsuite summary for yara 3.6.3
============================================================================
# TOTAL: 6
# PASS:  6
# SKIP:  0
# XFAIL: 0
# FAIL:  0
# XPASS: 0
# ERROR: 0
============================================================================
make[3]: Leaving directory '/home/admin1/yara-3.6.3'
make[2]: Leaving directory '/home/admin1/yara-3.6.3'
make[1]: Leaving directory '/home/admin1/yara-3.6.3'
admin1@admin1-virtual-machine:~/yara-3.6.3$ make check
```

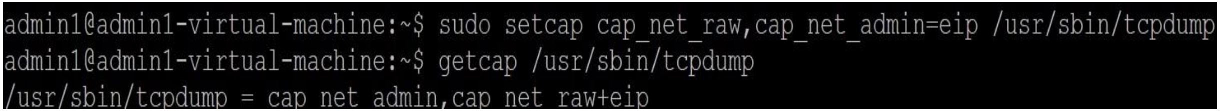
Cuckoo modified Installation

- Install pydeep



```
sudo apt-get install python-dev libfuzzy-dev
sudo git clone https://github.com/kbandla/pydeep.git
cd pydeep/
sudo python setup.py build
sudo python setup.py test
sudo python setup.py install
```

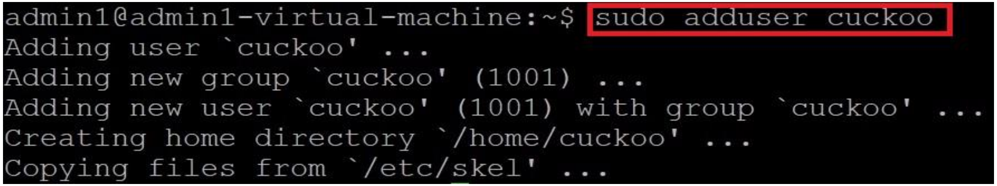
- Install tcpdump (installed by default in Ubuntu)
- Tcpdump requires root privileges, but since Cuckoo does not need to run as root set specific Linux capabilities to the binary



```
admin1@admin1-virtual-machine:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
admin1@admin1-virtual-machine:~$ getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

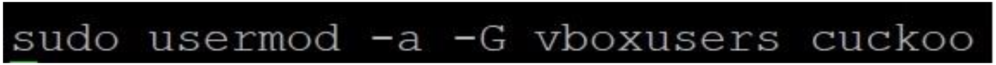
Cuckoo modified Installation

- Optional: Create a new user



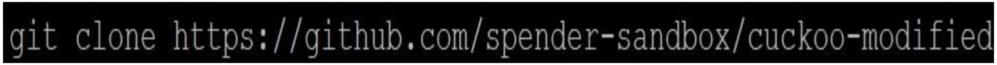
```
admin1@admin1-virtual-machine:~$ sudo adduser cuckoo
Adding user `cuckoo' ...
Adding new group `cuckoo' (1001) ...
Adding new user `cuckoo' (1001) with group `cuckoo' ...
Creating home directory `/home/cuckoo' ...
Copying files from `/etc/skel' ...
```

- If using VirtualBox add the new user to the vboxusers group

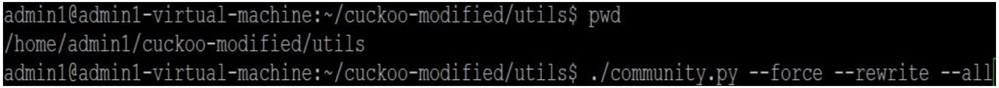


```
sudo usermod -a -G vboxusers cuckoo
```

- Install Cuckoo modified



```
git clone https://github.com/spender-sandbox/cuckoo-modified
```

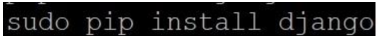


```
admin1@admin1-virtual-machine:~/cuckoo-modified/utils$ pwd
/home/admin1/cuckoo-modified/utils
admin1@admin1-virtual-machine:~/cuckoo-modified/utils$ ./community.py --force --rewrite --all
```

Cuckoo modified Installation

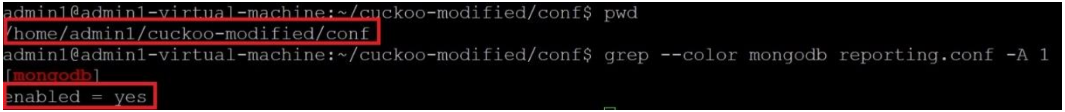
- Configure the web interface

◎ Install django



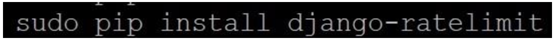
```
sudo pip install django
```

◎ Enable Mongodb

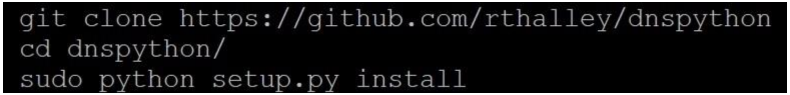


```
admin1@admin1-virtual-machine:~/cuckoo-modified/conf$ pwd
/home/admin1/cuckoo-modified/conf
admin1@admin1-virtual-machine:~/cuckoo-modified/conf$ grep --color mongodb reporting.conf -A 1
[mongodb]
enabled = yes
```

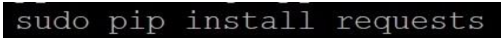
◎ Install missing modules



```
sudo pip install django-ratelimit
```



```
git clone https://github.com/rthalley/dnspython
cd dnspython/
sudo python setup.py install
```

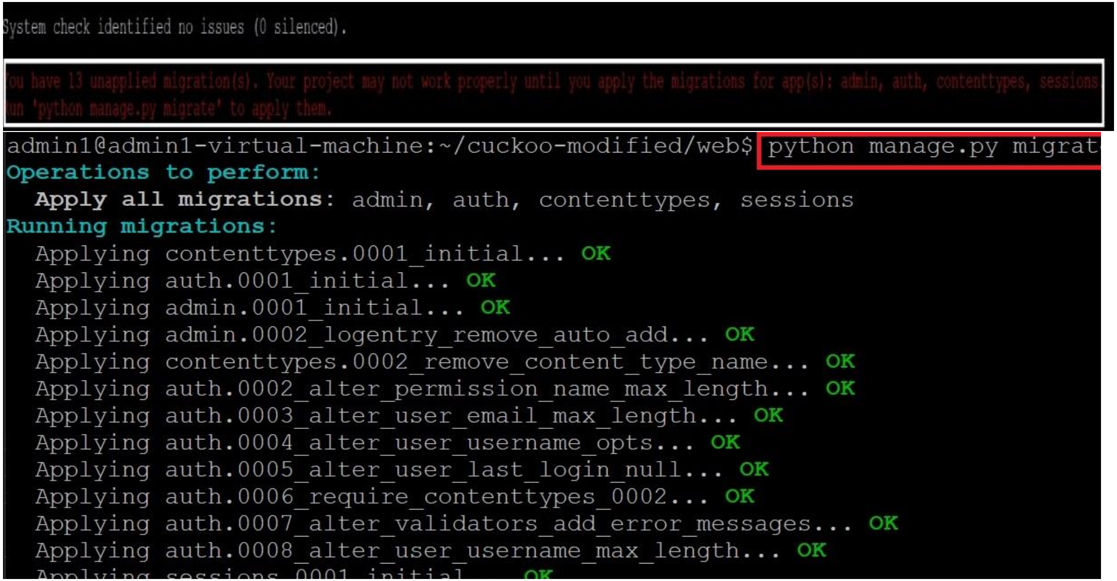


```
sudo pip install requests
```

Cuckoo modified Installation

- Configure the web interface

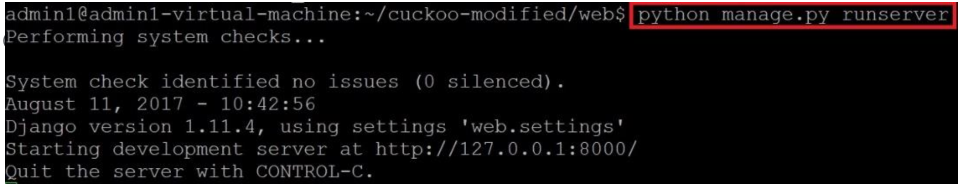
◎ Apply the migrations



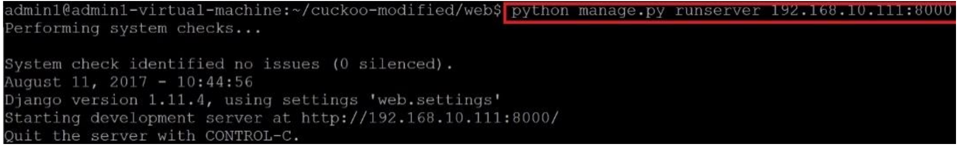
```
ystem check identified no issues (0 silenced).

ou have 13 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions
un 'python manage.py migrate' to apply them.
admin1@admin1-virtual-machine:~/cuckoo-modified/web$ python manage.py migrat
Operations to perform:
  Apply all migrations: admin, auth, contenttypes, sessions
Running migrations:
  Applying contenttypes.0001_initial... OK
  Applying auth.0001_initial... OK
  Applying admin.0001_initial... OK
  Applying admin.0002_logentry_remove_auto_add... OK
  Applying contenttypes.0002_remove_content_type_name... OK
  Applying auth.0002_alter_permission_name_max_length... OK
  Applying auth.0003_alter_user_email_max_length... OK
  Applying auth.0004_alter_user_username_opts... OK
  Applying auth.0005_alter_user_last_login_null... OK
  Applying auth.0006_require_contenttypes_0002... OK
  Applying auth.0007_alter_validators_add_error_messages... OK
  Applying auth.0008_alter_user_username_max_length... OK
  Applying sessions.0001_initial... OK
```

Cuckoo modified Installation

- Configure the web interface

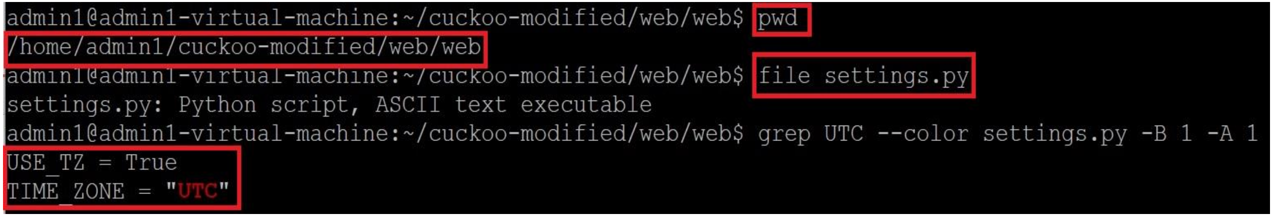


```
admin1@admin1-virtual-machine:~/cuckoo-modified/web$ python manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).
August 11, 2017 - 10:42:56
Django version 1.11.4, using settings 'web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```



```
admin1@admin1-virtual-machine:~/cuckoo-modified/web$ python manage.py runserver 192.168.10.111:8000
Performing system checks...

System check identified no issues (0 silenced).
August 11, 2017 - 10:44:56
Django version 1.11.4, using settings 'web.settings'
Starting development server at http://192.168.10.111:8000/
Quit the server with CONTROL-C.
```

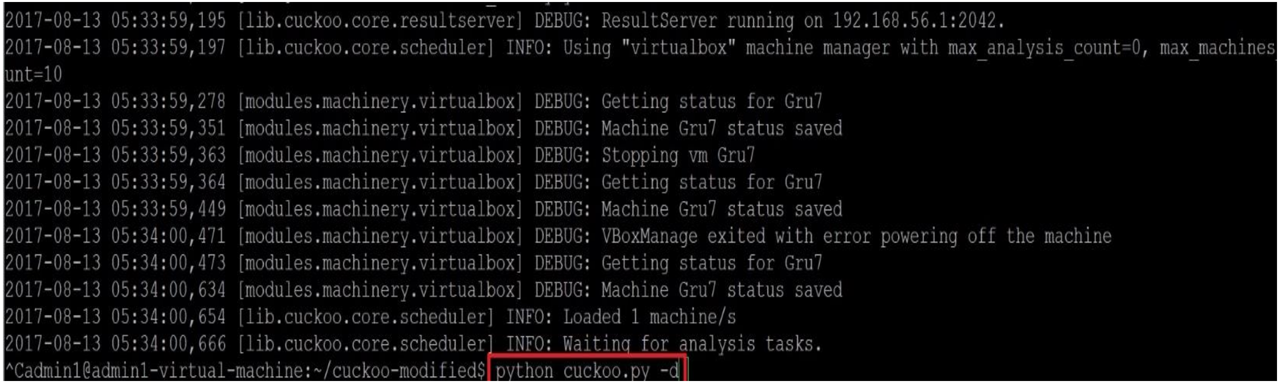
◎ Resolve /* NoneType' object has no attribute 'upper */ when starting the web interface



```
admin1@admin1-virtual-machine:~/cuckoo-modified/web/web$ pwd
/home/admin1/cuckoo-modified/web/web
admin1@admin1-virtual-machine:~/cuckoo-modified/web/web$ file settings.py
settings.py: Python script, ASCII text executable
admin1@admin1-virtual-machine:~/cuckoo-modified/web/web$ grep UTC --color settings.py -B 1 -A 1
USE_TZ = True
TIME_ZONE = "UTC"
```

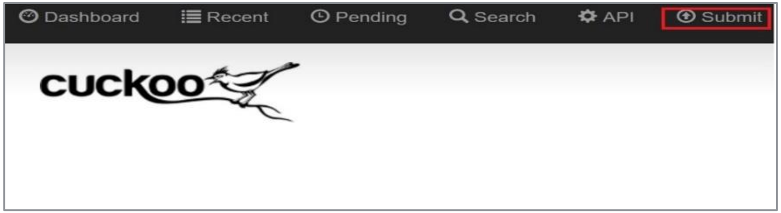
Submit a file through the web interfaces

- Run cuckoo



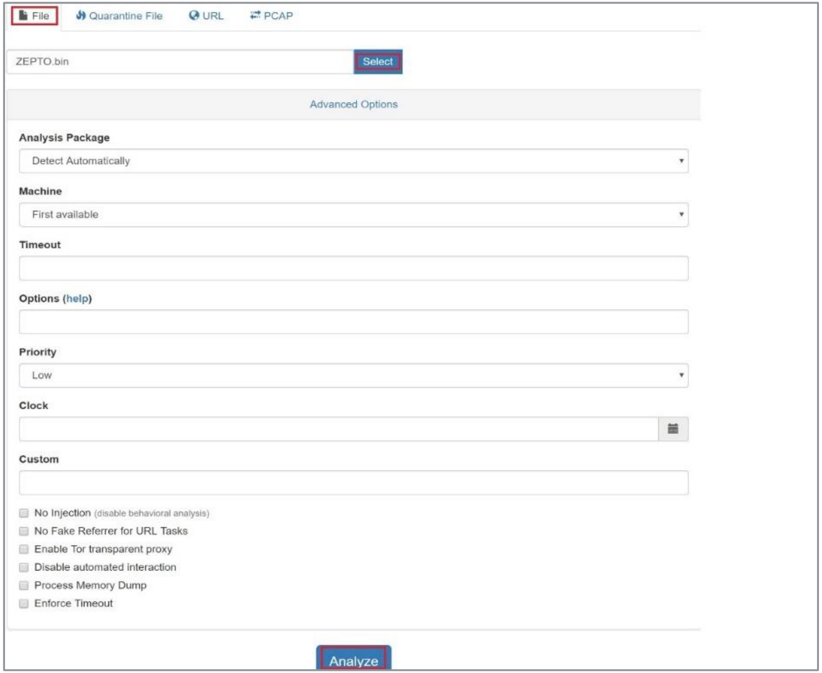
```
2017-08-13 05:33:59,195 [lib.cuckoo.core.resultserver] DEBUG: ResultServer running on 192.168.56.1:2042.
2017-08-13 05:33:59,197 [lib.cuckoo.core.scheduler] INFO: Using "virtualbox" machine manager with max_analysis_count=0, max_machines
unt=10
2017-08-13 05:33:59,278 [modules.machinery.virtualbox] DEBUG: Getting status for Gru7
2017-08-13 05:33:59,351 [modules.machinery.virtualbox] DEBUG: Machine Gru7 status saved
2017-08-13 05:33:59,363 [modules.machinery.virtualbox] DEBUG: Stopping vm Gru7
2017-08-13 05:33:59,364 [modules.machinery.virtualbox] DEBUG: Getting status for Gru7
2017-08-13 05:33:59,449 [modules.machinery.virtualbox] DEBUG: Machine Gru7 status saved
2017-08-13 05:34:00,471 [modules.machinery.virtualbox] DEBUG: VBoxManage exited with error powering off the machine
2017-08-13 05:34:00,473 [modules.machinery.virtualbox] DEBUG: Getting status for Gru7
2017-08-13 05:34:00,634 [modules.machinery.virtualbox] DEBUG: Machine Gru7 status saved
2017-08-13 05:34:00,654 [lib.cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2017-08-13 05:34:00,666 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
^Cadmin1@admin1-virtual-machine:~/cuckoo-modified$ python cuckoo.py -d
```

- Submit a file



Submit a file through the web interfaces

- Submit a file



ZEPTO.bin

Analysis Package
Detect Automatically

Machine
First available

Timeout

Options (help)

Priority
Low

Clock

Custom

□ No Injection (disable behavioral analysis)
□ No Fake Referrer for URL Tasks
□ Enable Tor transparent proxy
□ Disable automated interaction
□ Process Memory Dump
□ Enforce Timeout

References

- Cuckoo website

https://cuckoosandbox.org

- GitHub

https://github.com/cuckoosandbox/cuckoo

- Cuckoo modified Github

https://github.com/spender-sandbox/cuckoo-modified