W2RC & W3RS INSTALLATION GUIDE

2019

OVERVIEW

1. Setting up the environment

Requirements

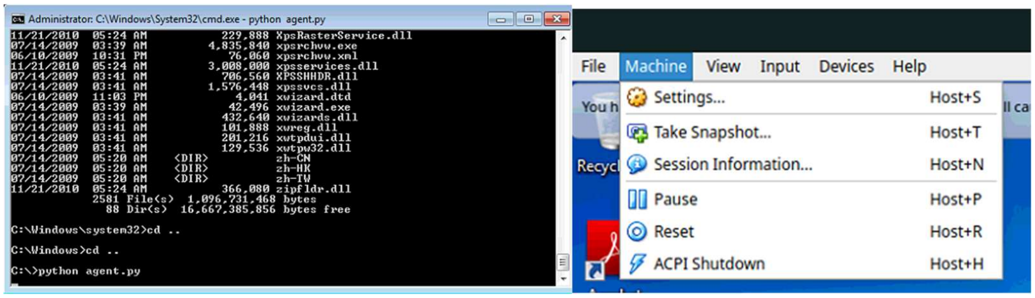
- ***Python 3.7** (sudo apt-get install python3.7 python3.7-venv)*
- ***Virtual Box (Windows VM) (https://www.virtualbox.org/wiki/Downloads)***
- ***MongoDB (https://docs.mongodb.com/manual/installation/)***
- ***Cuckoo Framework (https://cuckoosandbox.org/) – Guided in Step 3***

It is recommended that a Linux system should be used for the analysis server in order to ensure better performance and added security. Ensure all system packages are up to date prior to installation. It is not recommended to install the systems in a Virtual machine due to degraded performance and having virtualization within virtualization which is not recommended and has many limitations. Installing python is essential for the system to work as well as the above-mentioned packages. Following this guide will give you the basics on how to setup cuckoo and prepare the system for the Ransomware Readiness Framework (R^{2}F). A detailed guide on how to setup cuckoo is available on their doc's page (https://cuckoo.readthedocs.io/en/latest/installation/). However, step 3 of this guide will help you install and configure the necessary requirements to get the system working. The next step will focus on creating a VM and configuring it.

2. Setting up Virtual Box

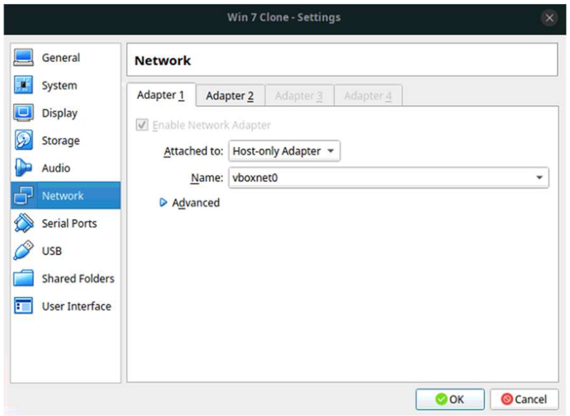
Create a Windows VM

In order to analyse executables, a Windows VM needs to be created. You are not only limited to Virtual Box other platforms like VMWare, QEMU and KVM are supported. For the sake of simplicity and open-source nature of these prototypes, Virtual Box will be used. Due to Window Licensing, you will need to create this VM on your own using an ISO or preconfigured VM obtainable from Microsoft. The system specifications are up to you to decide. It is recommended to use at least 2GB of memory however with an increase in memory there is also an increase in the time it takes to analyse a sample. In order to allow the VM to communicate to the analysis engine, the agent needs to be run in the VM. Download and install python on the VM and ensure you install the pillow python package **$> pip install pillow** this allows the agent the ability to take screenshots of the VM which help an investigator to see what is happening in the background. After python is installed download the agent (https://github.com/cuckoosandbox/cuckoo/blob/master/cuckoo/data/agent/agent.py) and run it with Administrator privileges. No output will be shown but once the script is running.


Administrator: C:\Windows\System32\cmd.exe - python agent.py

```
11/21/2010  05:24 AM           229,888 XpsRasterService.dll
07/14/2009  03:39 AM         4,835,840 xpsrchvw.exe
06/10/2009  10:31 PM            76,060 xpsrchvw.xml
11/21/2010  05:24 AM         3,008,000 xpsservices.dll
07/14/2009  03:41 AM           706,560 XPSSHHDR.dll
07/14/2009  03:41 AM         1,576,448 xpssvcs.dll
06/10/2009  11:03 PM             4,041 xwizard.dtd
07/14/2009  03:39 AM            42,496 xwizard.exe
07/14/2009  03:41 AM           432,640 xwizards.dll
07/14/2009  03:41 AM           101,888 xwreg.dll
07/14/2009  03:41 AM           201,216 xwtpdui.dll
07/14/2009  03:41 AM           129,536 xwtpw32.dll
07/14/2009  05:20 AM    <DIR>          zh-CN
07/14/2009  05:20 AM    <DIR>          zh-HK
07/14/2009  05:20 AM    <DIR>          zh-TW
11/21/2010  05:24 AM           366,080 zipfldr.dll
            2581 File(s)  1,096,731,468 bytes
              88 Dir(s)  16,667,385,856 bytes free

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>python agent.py
```

Take a snapshot of the machine while the agent is running. This is important as this snapshot will be used for performing analysis. More information on how to correctly configure the agent is available here (https://cuckoo.readthedocs.io/en/latest/installation/guest/agent/). Ensure that your VM uses the Host-Only adapter and that the adapter is configured on the same subnet as the physical machine.



Win 7 Clone - Settings

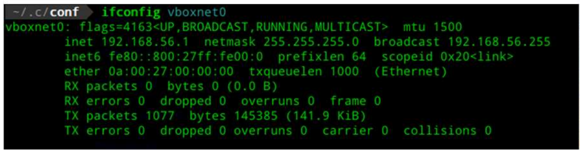
Network

☑ Enable Network Adapter

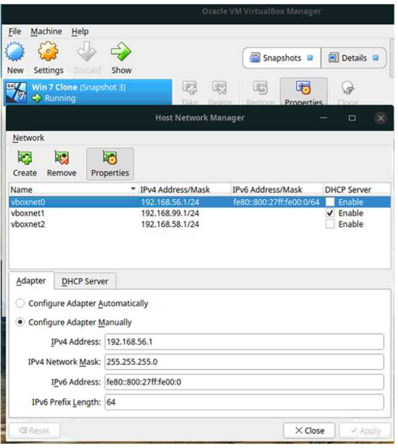
Attached to: Host-only Adapter

Name: vboxnet0

Setting the IP address of the host can be found on the setting of the VM under the network tab. Furthermore, setting the VirtualBox Host manager can be done from the main Virtual Box Menu -> File -> Host Network Manager. The screenshot below shows how to correctly set up the manager. Ensure that the gateway IP address matches that of cuckoo (note down the IP address so it can be added to the cuckoo configuration in step 3) and it matches vboxnet0 system, network manager. Please make sure that the DHCP Server is unchecked, this prevents Virtual Box from trying to assign an IP address using the NAT adapter from the system. This is because the cuckoo framework does not support DHCP.



```
~/.c/conf  ifconfig vboxnet0
vboxnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::800:27ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        ether 0a:00:27:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1077  bytes 145385 (141.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Oracle VM VirtualBox Manager

Win 7 Clone (Snapshot 3)
Running

Host Network Manager

Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
vboxnet0	192.168.56.1/24	fe80::800:27ff:fe00:0/64	□ Enable
vboxnet1	192.168.99.1/24		☑ Enable
vboxnet2	192.168.58.1/24		□ Enable

○ Configure Adapter Automatically

● Configure Adapter Manually

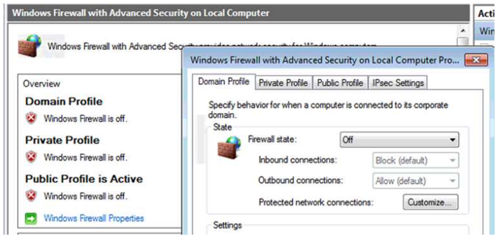
IPv4 Address: 192.168.56.1

IPv4 Network Mask: 255.255.255.0

IPv6 Address: fe80::800:27ff:fe00:0

IPv6 Prefix Length: 64

It is recommended that other general software also is installed and configured appropriately like Adobe Reader, Microsoft Office, etc. Be sure to disable auto-updates of this software. Disable the firewall and anti-virus in the VM also any auto-updates.



Windows Firewall with Advanced Security on Local Computer

Overview

Domain Profile
Windows Firewall is off.

Private Profile
Windows Firewall is off.

Public Profile is Active
Windows Firewall is off.

Windows Firewall Properties

Windows Firewall with Advanced Security on Local Computer Pro...

Specify behavior for when a computer is connected to its corporate domain.

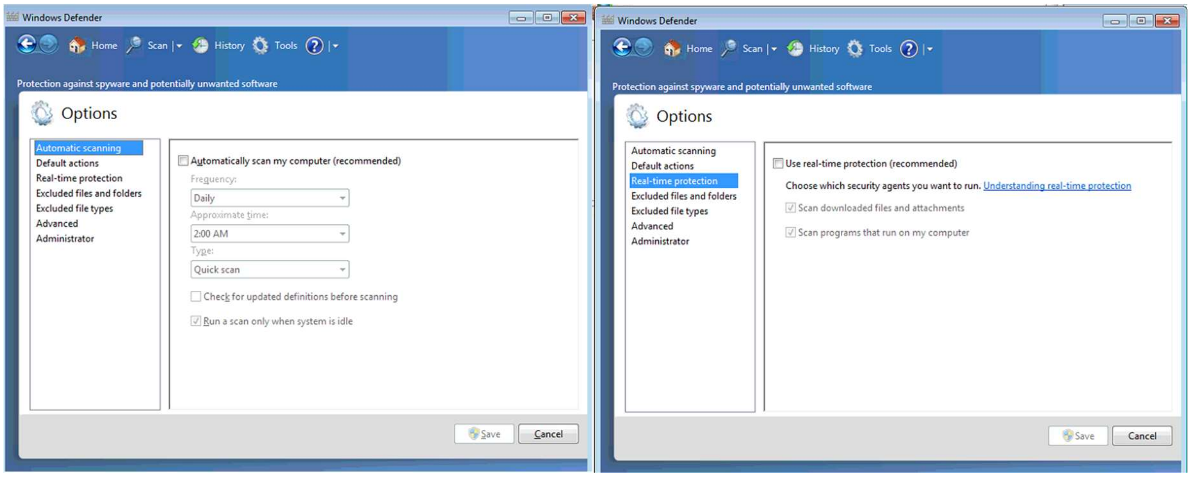
State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:


Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
Save
Cancel

Options

Automatic scanning
Default actions
Real-time protection
Excluded files and folders
Excluded file types
Advanced
Administrator

□ Automatically scan my computer (recommended)

Frequency: Daily

Approximate time: 2:00 AM

Type: Quick scan

□ Check for updated definitions before scanning

☑ Run a scan only when system is idle

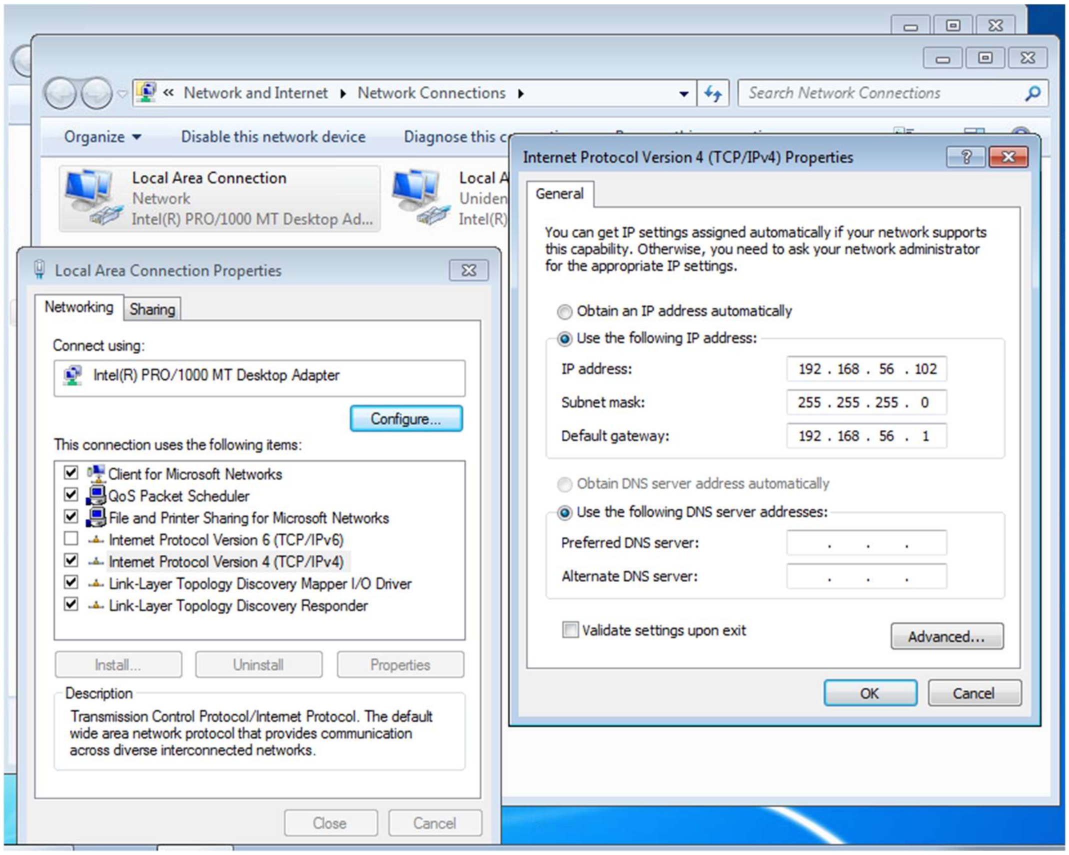
□ Use real-time protection (recommended)

Choose which security agents you want to run. Understanding real-time protection

☑ Scan downloaded files and attachments

☑ Scan programs that run on my computer

This is vital otherwise this may hinder analysis and block the agent from communicating to the server. In order to correctly allow your VM to communicate with the cuckoo server, the network adapter inside the VM in Windows needs to change to be a static IP instead of DHCP as this is not supported by cuckoo and will break the entire analysis process. Navigate to “**Control Panel\Network and Internet\Network Connections**” right-click on the network adapter -> properties -> navigate to the IPv4 -> properties and change from “Obtain an IP address automatically” to “Use the following IP address” as indicated in the screenshot below. Assign the machine the IP address you want and note it down as this will be the same IP address you provide to the cuckoo configuration in step 3



Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 56 . 102

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 56 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

3. Setting up Cuckoo Framework

> *Cuckoo framework is a bit tedious to setup but once everything is configured correctly it provides a powerful platform. Please ensure you follow these instructions carefully*

It is recommended that you run cuckoo under its own user and therefore you must create a user called cuckoo you can find the installation process for that here (https://cuckoo.readthedocs.io/en/latest/installation/host/installation/). Create a python virtual environment for cuckoo to run in, this is to ensure that nothing bad will happen to the system and ensures that cuckoo remains compatible even if system packages are updated. To sum it up run the following commands:

```
#Creating a cuckoo user
$ sudo adduser cuckoo
$ sudo usermod -a -G vboxusers cuckoo
$ sudo usermod -a -G libvirtd cuckoo

#Installing cuckoo in a venv
$ virtualenv venv                        # This creates a virtualized environment
$ source venv/bin/activate               # This enters into python virtual environment
(venv)$ pip install -U pip setuptools
(venv)$ pip install -U cuckoo
(venv)$ cuckoo -d                        # This will now create cuckoo configuration files
```

In order to simplify the package installation process, you can clone or download the W3RS(https://github.com/AvinashSingh786/W3RS) repositories and navigate into the directory and run the command in the virtual environment.

```
(venv)$ pip install -r requirements.txt
```

After cuckoo configurations have been created they can be found in the CWD of cuckoo which is `~/.cuckoo`

Open the file `~/.cuckoo/config/cuckoo.conf` and ensure the information there is correct and matches the config below:

```
machinery = virtualbox
ip = 192.168.56.1                  # IP address of Windows VM gateway (same as system adapter vboxnet0)
```

For larger processing of analysis, you can use your own database and can configure it in the [database] section, if not a default SQLite DB will be created.

Open the file `~/.cuckoo/config/auxilary.conf` and ensure the information there is correct and matches the config below:

```
[sniffer]
enabled = yes                      # Ensure that tcpdump is installed
tcpdump = /usr/sbin/tcpdump        # Path to tcpdump installation binary
```

This is to monitor network connections and any outgoing requests are logged for trackability as well as investigative processes.

Open the file `~/.cuckoo/config/memory.conf` and ensure the information there is correct and matches the config below:

NB: ensure that volatility is installed (**(venv)$ pip install volatility**)

Ensure that all the plugins are enabled in this configuration as this analysis's memory information one of the vital parts for the framework and potential recovery from a ransomware attack. Set the "guest_profile" variable to the profile that matches your Windows VM to prevent wasting time identifying the profile. A list of profiles can be found here (https://github.com/volatilityfoundation/volatility/wiki/2.6-Win-Profiles).

Open the file `~/.cuckoo/config/processing.conf` and ensure the information there is correct and matches the config below:

```
    [analysisinfo]
        enabled = yes
    [behavior]
        enabled = yes
    [buffer]
        enabled = yes
    [strings]
        enabled = yes
    [static]
        enabled = yes
   [procmemory]
        enabled = yes
```

Open the file `~/.cuckoo/config/reporting.conf` and ensure the information there is correct and matches the config below:

NB: Ensure that is correct as this is a vital part in determining the maliciousness of a process.

```
   [jsondump]
       enabled = yes
       indent = 4
       calls = yes
   [mongodb]
        enabled = yes
        host = 127.0.0.1
        port = 27017
        db = cuckoo
        store_memdump = yes
        paginate = 100
        # MongoDB authentication (optional).
        username = root
        password = password
```

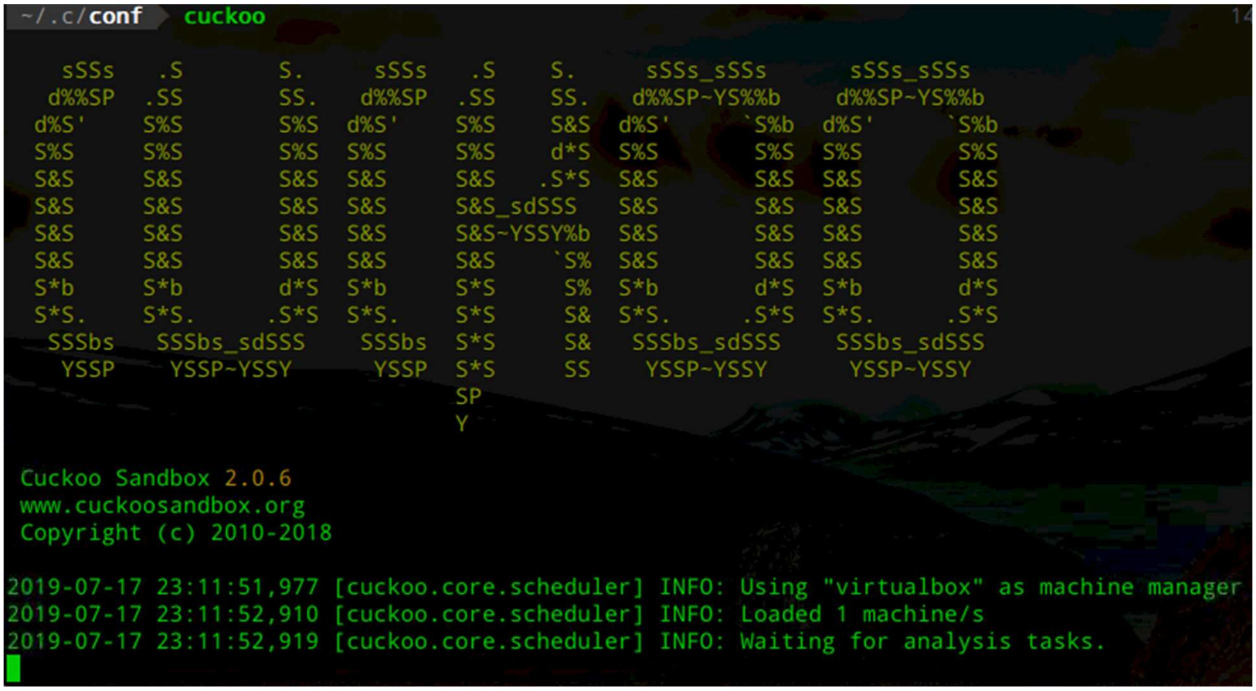
Ensure that a database is created in MongoDB and that the login details are correct, note that they are optional.

Open the file `~/.cuckoo/config/virtualbox.conf` and ensure the information there is correct and matches the config below:

```
   [virtualbox]
        mode = headless
        path = /usr/bin/VBoxManage       # Path to the local installation of the VBoxManage utility.
        interface = vboxnet0
        machines = cuckoo1
    [cuckoo1]
        label = Win 7                  # Specify the label name of the current machine as specified in your
        platform = windows
        ip = 192.168.56.102            # 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.
        snapshot = Snapshot 1          # Name of the snapshot taken in step 2
```

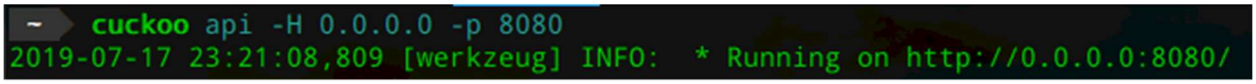
More details on how to configure other services and configurations can be found on the cuckoo config docs page (https://cuckoo.readthedocs.io/en/latest/installation/host/configuration/#cuckoo-conf)

To ensure that everything is correctly setup within the (venv) run the cuckoo command "**(venv)$ cuckoo**" you should see something similar to the screenshot below:



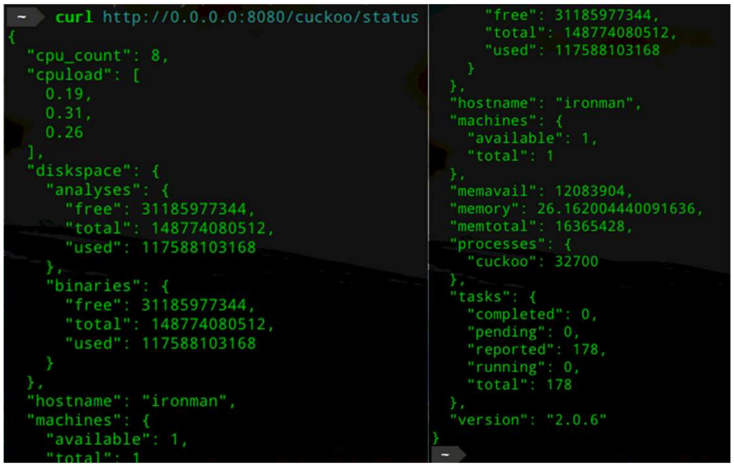
```
~/.c/conf  cuckoo

    sSSs   .S       S.     sSSs   .S    S.     sSSs_sSSs      sSSs_sSSs
   d%%SP  .SS       SS.   d%%SP  .SS    SS.   d%%SP~YS%%b    d%%SP~YS%%b
  d%S'    S%S       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    d*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_sdSSS   S&S        S&S  S&S        S&S
  S&S     S&S       S&S  S&S     S&S~YSSY%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*b     S*b       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
                                 SP
                                 Y

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

2019-07-17 23:11:51,977 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2019-07-17 23:11:52,910 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2019-07-17 23:11:52,919 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
```

The cuckoo server is now ready to receive analysis tasks. In order to make cuckoo accessible to other clients (W2RC), the cuckoo API needs to be executed in a different terminal tab with the command **(venv)$ cuckoo api -H 0.0.0.0 -p 8080**



```
~  cuckoo api -H 0.0.0.0 -p 8080
2019-07-17 23:21:08,809 [werkzeug] INFO:  * Running on http://0.0.0.0:8080/
```

NB. Note that it serves on 0.0.0.0 this means that is accessible by the systems IP assigned through the network. To test that it works check your IP from "ifconfig" and perform a curl request on the path "/cuckoo/status" like in the screenshot below:



```
~ curl http://0.0.0.0:8080/cuckoo/status
{
  "cpu_count": 8,
  "cpuload": [
    0.19,
    0.31,
    0.26
  ],
  "diskspace": {
    "analyses": {
      "free": 31185977344,
      "total": 148774080512,
      "used": 117588103168
    },
    "binaries": {
      "free": 31185977344,
      "total": 148774080512,
      "used": 117588103168
    }
  },
  "hostname": "ironman",
  "machines": {
    "available": 1,
    "total": 1
```

```
      "free": 31185977344,
      "total": 148774080512,
      "used": 117588103168
    }
  },
  "hostname": "ironman",
  "machines": {
    "available": 1,
    "total": 1
  },
  "memavail": 12083904,
  "memory": 26.162004440091636,
  "memtotal": 16365428,
  "processes": {
    "cuckoo": 32700
  },
  "tasks": {
    "completed": 0,
    "pending": 0,
    "reported": 178,
    "running": 0,
    "total": 178
  },
  "version": "2.0.6"
}
~
```

This provides the status of the machine as well as some statistics if you get output similar to the screenshots above that means the API is running successfully. The next step is to set up a secure storage engine W3RS.

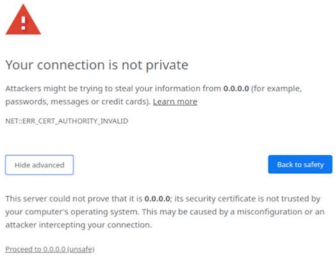
4. Setting up Storage (W3RS)

Ensure that the relevant python packages are installed

If not done already clone or download the repository https://github.com/AvinashSingh786/W3RS. It is recommended to create a separate python virtual environment and serve it in the directory /srv/W3RS/venv using the same commands listed in Step 3. You will then also have to install any python packages from the requirements.txt file. Since this application uses Django it can also be configured using uwsgi but the sake of simplicity we will use Django's inbuilt server functionality. In the virtual environment run the following commands:

```
#Installing W3RS in a venv
$ virtualenv venv -p python3              # This creates a virtualized environment
$ source venv/bin/activate                # This enters into python virtual environment
(venv)$ pip install -r requirements.txt
(venv)$ python manage.py createsuperuser  # Create a super user that you will use as the admin
(venv)$ python manage.py makemigrations   # This sets up the storage engine and databases
(venv)$ python manage.py migrate          # This creates the databases and interfaces
(venv)$ python manage.py runsslserver 0.0.0.0:8000
```

The last command will run a secure SSL server on port 8000, note that this will use a self-signed certificate and will not be shown as safe in the browser. In order to prevent that you will need to get an SSL certificate from a Certificate Company. If you don't want the unsafe https to be displayed in the browser, you can obtain an SSL certificate from Let's Encrypt CA (`https://letsencrypt.org/`). You will get crt or pem files and you can just supply the path to these files with the following flags ***--certificate*** and **--key** when running the SSL server. Once the server is running to ensure that the setup has completed correctly navigate to the link provided from the command and check if you get a screenshot similar to the one below. Having an SSL server protects the traffic being transferred from clear text attacks and network sniffing. Navigate to https://0.0.0.0:8000 got to advanced and proceed to site.



Your connection is not private

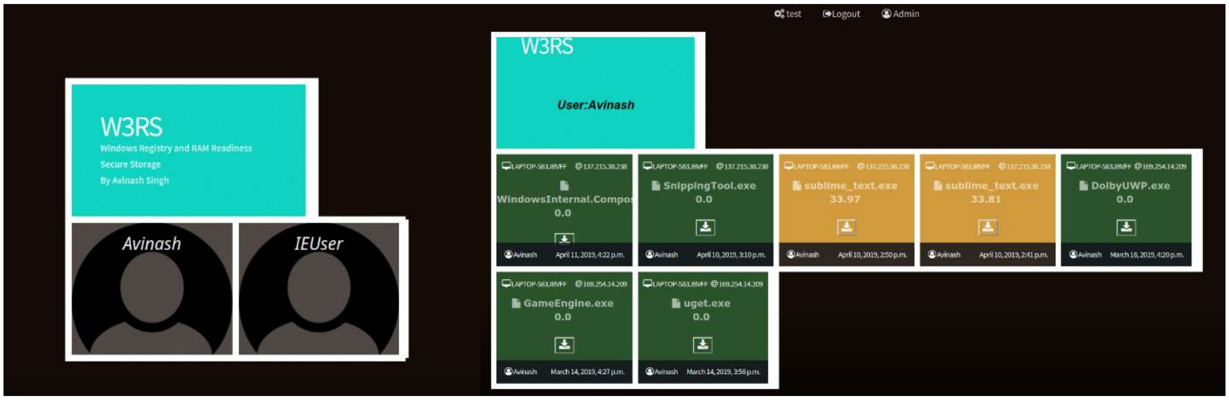
Attackers might be trying to steal your information from **0.0.0.0** (for example, passwords, messages or credit cards). Learn more

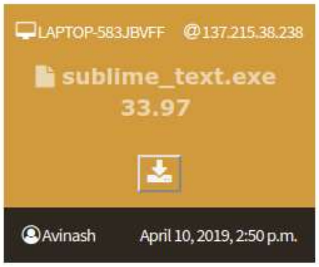
NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **0.0.0.0**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 0.0.0.0 (unsafe)

In order to download PDE, you will need to enable 2-factor authentication. In order to do that you will need to be logged in. After you have logged in with the superuser details you can choose your method of 2FA for simplicity, take the default option. Use the mobile app Authy or Google Authenticator to scan the QR code presented on the next screen and enter in the 6-digit token from the app and 2FA will be enabled. You can visit your profile page and create backup tokens however this is not advised. In order to enable email notifications, navigate to W3RS -> settings.py and replace the EMAIL details section with the relevant information. Once you are done setting up you will see a blank screen but once the W2RC is set up you will see something similar to the screenshot below and once the desired user is clicked the collection of analysed samples will be shown:


W3RS
Windows Registry and RAM Readiness
Secure Storage
By Avinash Singh
Avinash
IEUser
test
Logout
Admin
W3RS
User:Avinash
LAPTOP-583JBVFF @137.215.38.238
WindowsInternal.Compo
0.0
Avinash April 11, 2019, 4:22 p.m.
LAPTOP-583JBVFF @137.215.38.238
SnippingTool.exe
0.0
Avinash April 10, 2019, 3:10 p.m.
LAPTOP-583JBVFF @137.215.38.238
sublime_text.exe
33.97
Avinash April 10, 2019, 2:50 p.m.
LAPTOP-583JBVFF @137.215.38.238
sublime_text.exe
33.81
Avinash April 10, 2019, 2:41 p.m.
LAPTOP-583JBVFF @169.254.14.209
DolbyUWP.exe
0.0
Avinash March 18, 2019, 4:20 p.m.
LAPTOP-583JBVFF @169.254.14.209
GameEngine.exe
0.0
Avinash March 14, 2019, 4:27 p.m.
LAPTOP-583JBVFF @169.254.14.209
uget.exe
0.0
Avinash March 14, 2019, 3:56 p.m.


LAPTOP-583JBVFF @137.215.38.238
sublime_text.exe
33.97
Avinash April 10, 2019, 2:50 p.m.

When analysing the information about the executable we see the machine name ("LAPTOP-533JBVFF") and the IP address of the machine on the top right as well as the executable name in the center. The CAT value is shown in the middle with the download PDE button that will allow the JSON encoded PDE to be downloaded and further analysed. The user of the machine and the date and time appear at the bottom in case the machine has multiple users and the date and time it for reliability purposes.

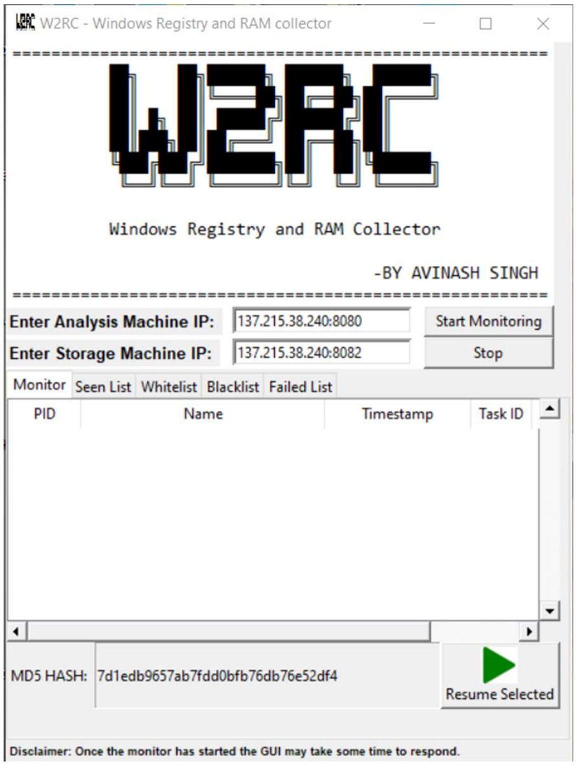
After the storage engine has been setup the next step will be to setup the client on the user machines.

5. Setting up Collection (W2RC)

Requirement:
- OpenSSL – this is used for the https connection to the storage server W3RS

This tool is packaged in an MSI file to ease the installation process on the client-side and removes the need to install additional libraries, etc.

W2RC can be downloaded from the releases page (https://github.com/AvinashSingh786/W2RC/releases) and installed on the user pc that wishes to be monitored using this framework. Run the executable and follow the instructions. Once the tool is installed an icon will be displayed on the desktop, edit this shortcut to "Run as Administrator". The tool needs to run as an administrator because it will be collecting information and sending executables for analysis. Run the tool and you should get a GUI interface like the screenshot below:



Enter Analysis Machine IP: 137.215.38.240:8080

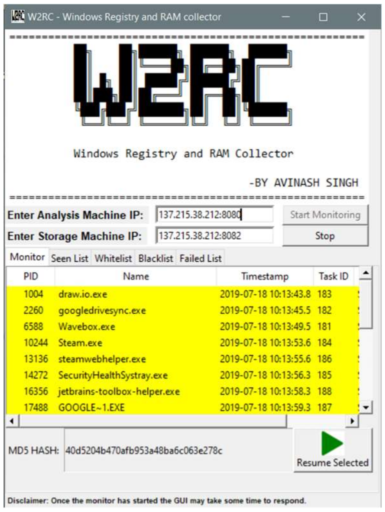
Enter Storage Machine IP: 137.215.38.240:8082

PID	Name	Timestamp	Task ID

MD5 HASH: 7d1edb9657ab7fdd0bfb76db76e52df4

Disclaimer: Once the monitor has started the GUI may take some time to respond.

In order to start the monitoring and collection tool W2RC, you will need to enter in the correct IP address or domain name of the server. The analysis machine IP is for the cuckoo API that was set up in step 3 and the storage machine IP is for the W3RS system. Ensure the ports are correct otherwise monitoring will not start and an error message will be shown. Logs are collected for the tool and can be found in the installation directory in program files. Once the tool detects that the 2 servers are online it will begin monitoring all processes on the system. Since this is just a prototype too there are some inefficiencies and bugs. For start, once the monitoring has started the GUI may become a bit unresponsive this is because of python not truly having concurrency but rather simulated. This, therefore, relies on the main thread to switch between child threads which takes some time due to the constant monitoring of the processes. In order to ensure the integrity of the databases for seen processes, whitelisted and blacklisted the MD5 sum of each database is shown at the bottom as well as in the logs further ensuring integrity when questioned. Once the monitor has started it will find processes that have not been seen before and send the executable to the analysis machine. Below is a screenshot of the working of W2RC.



Enter Analysis Machine IP: 137.215.38.212:8080

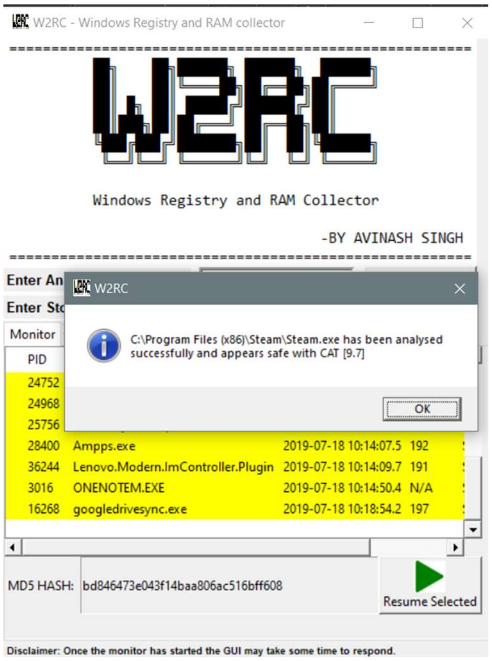
Enter Storage Machine IP: 137.215.38.212:8082

PID	Name	Timestamp	Task ID
1004	draw.io.exe	2019-07-18 10:13:43.8	183
2260	googledrivesync.exe	2019-07-18 10:13:45.5	182
6588	Wavebox.exe	2019-07-18 10:13:49.5	181
10244	Steam.exe	2019-07-18 10:13:53.6	184
13136	steamwebhelper.exe	2019-07-18 10:13:55.6	186
14272	SecurityHealthSystray.exe	2019-07-18 10:13:56.3	185
16356	jetbrains-toolbox-helper.exe	2019-07-18 10:13:58.3	188
17488	GOOGLE~1.EXE	2019-07-18 10:13:59.3	187

MD5 HASH: 40d5204b470afb953a48ba6c063e278c

Disclaimer: Once the monitor has started the GUI may take some time to respond.

The tool relies on both static and dynamic analysis, therefore if the behaviour of the executable cannot be determined at this stage the tool will report that it failed to determine the behaviour of the executable and will perform calculations and analysis using static methods. Once a process has been analysed and the CAT value determined it will be alerted to the user as in the screenshot below:



```
=======================================================
W2RC

Windows Registry and RAM Collector

                          -BY AVINASH SINGH
=======================================================
```

C:\Program Files (x86)\Steam\Steam.exe has been analysed successfully and appears safe with CAT [9.7]

PID			
24752			
24968			
25756			
28400	Ampps.exe	2019-07-18 10:14:07.5	192
36244	Lenovo.Modern.ImController.Plugin	2019-07-18 10:14:09.7	191
3016	ONENOTEM.EXE	2019-07-18 10:14:50.4	N/A
16268	googledrivesync.exe	2019-07-18 10:18:54.2	197

MD5 HASH: bd846473e043f14baa806ac516bff608

Disclaimer: Once the monitor has started the GUI may take some time to respond.

All unseen processes will be quickly suspended, and the process will undergo analysis to determine if it is benign or malicious once the result comes back the process is resumed or killed.

THANK YOU 😉

Installation guide created by ***Avinash Singh***
Date: 2019/07/18
Contact: asingh@cs.up.ac.za