**Cuckoo Installation**

**Prerequisites:**

* OS: Ubuntu 20.04 (<https://releases.ubuntu.com/20.04/>)
* RAM: 16 GB recommended
* Storage: 500 GB (will depend on usecase)
* Internet Connection
* Avoid the name “cuckoo” as usernames to avoid conflicts with below commands.
* If Ubuntu is in a VM, make sure VT-x is compatible and enabled.
* Enable Virtualization from BIOS/UEFI (Maybe labelled as VT-x, VT-d or AMD-v or Virtualization Technology)
* Windows 7 64-bit
  + ISO Download: https://getintopc.com/softwares/operating-systems/windows-7-ultimate-32-64-bit-updated-aug-2020-download-1747331/?id=000265748703
  + Activation Keys: [https://gist.github.com/jerodg/502bd80a715347662e79af526c98f187#windows-7](https://gist.github.com/jerodg/502bd80a715347662e79af526c98f187" \l "windows-7)
  + Alternate Activation: <https://gist.github.com/jsakhil/b7a4a6b64ff195232364fa7b59c47b21>

**Cuckoo Installation Steps:**

* Boot into Ubuntu
* Clone or Download this repository (<https://github.com/ezyway/Cuckoo-Scripts>)
* Execute “cuckoo\_install\_script\_minimal.sh”
* VM Windows Installation and Configuration
  + Install Windows 7 on the Virtual Machine with the following specs:
    - VM Label: win7x64
    - OS used here: Windows 7 Ultimate x64
    - RAM: 2 GB (memory dump will be of 2 GB for each analysis) [can be set to 1GB]
    - NETWORK: NAT (Switch to Host Only Adapter when analysis starts)
    - CPU: 4 (i5 8300H has 8 logical cores; Use half of your cpu’s core)
    - Storage Size: 32 GB [use fixed type for better performance]
  + Boot to Windows 7
  + To disable forced signed driver installation in x64 windows, launch command prompt as admin and execute:
    - bcdedit -set TESTSIGNING ON
    - If the command throws an error, skip this part and move on.
  + In VM toolbar, go to, Devices --> Insert Guest Additions CD Image
  + Go to Windows 7 and install VirtualBox Guest Additions and Reboot
  + Open run dialog (Win+R) and type ‘gpedit.msc’:
    - Expand Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. Scroll down to the User Account Control options:
      * Right click the “User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode” and select Properties. Using the drop-down menu select Elevate without prompting and click ok.
      * Right click the “User Account Control: Detect application installations and prompt for elevation” and select Properties. Check the Disabled option and click ok.
      * Right click the “User Account Control: Run all administrators in Admin Approval Mode” and select Properties. Check the Disabled option and click ok.
    - Disable the automatic install of Windows Updates: Computer Configuration > Administrative Templates > Windows Components > Windows Update and right click Configure Automatic Updates and edit. Select Enabled, 2- Notify for download and notify for install, then click ok.
    - Disable Firewall: Computer Configuration > Administrative Templates > Network > Network connections > Windows Firewall > Domain Profile > Windows Firewall and change “Protect all network connections” to Disabled.
    - Disable Windows Defender: Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus then set “Turn off Windows Defender Antivirus” to Enabled.

* + In VM window, go to Settings > Shared Folders, and create a shared folder (move files from Ubuntu to Windows).
  + Place the following files in the Shared Folder in Ubuntu:
    - Python 2.7: <https://www.python.org/ftp/python/2.7.8/python-2.7.8.amd64.msi>
    - Pillow 2.5.3: <https://pypi.python.org/packages/2.7/P/Pillow/Pillow-2.5.3.win-amd64-py2.7.exe>
    - Agent.py: /home/<username>/.cuckoo/agent/agent.py
    - Any other files to make the VM look like an authentic target. (MS Office 2013, Java, Flash, Acrobat Reader)
  + Access the folder in Windows 7 by going to \\vboxsvr\ in the network and:
    - Install all programs
    - Move agent.py to “C:\Users\***\*USERNAME\****\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup”

(Show Hidden Files: **Organize ->Folder Options->View->Show Hidden files, folders and drives**)

(Moving is optional as snapshot will have agent.py running)

* + Activate Windows (Optional) (<https://github.com/DEAM0/Windows-7-Activator> : Run the .bat file)
  + Reboot Windows and if network popup appears, click allow.
  + In VirtualBox, change Windows 7 VM Network Adapter to Host Only Adapter and select vboxnet0 as interface
  + In Windows 7, go to Adapter Settings (Start > Control Panel > Network and Sharing Center > Change adapter settings > Properties > Properties > Internet Protocol Version 4 (TCP/IPv4) Properties), set the following values after selecting “Use the following IP address:”:
    - IP Address: 192.168.56.101
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.56.1
    - Preferred DNS Server: 8.8.8.8

* + Disable and then Enable the Network Adapter
  + Perform ‘ping google.com’ to confirm internet access
  + Make sure ‘agent.py’ is running (blank command prompt)
  + Ensure output when ‘curl 192.168.56.101:8000’ is executed in Ubuntu
  + Start 2 or 3 applications (to appear like a normal victim in the middle of her/his work)
  + Take a snapshot, VM Window: Machines > Snapshot, name it machine\_ready\_snapshot
  + Shut Down Windows VM.
* Configuring Cuckoo (Follow ‘a’ or ‘b’)
  1. Copy conf/ from (<https://github.com/ezyway/Cuckoo-Scripts>) and paste it in ~.cuckoo/

**OR**

* 1. Go to ~/.cuckoo/conf
     + sudo nano cuckoo.conf

set: machinery = virtualbox

memory\_dump = yes

terminate\_processes = yes

free\_space = 4096

[resultserver] ip = 192.168.56.1

[cuckoo] version\_check = no

* + - sudo nano virtualbox.conf

set: mode = gui

label = win7x64

platform = windows

ip = 192.168.56.101

* + - sudo nano processing.conf

set: [memory] enabled = yes

* + - sudo nano memory.conf

set: guest\_profile = Win7SP1x64 (If other OS, find profile by: vol.py --info |grep Profiles -A48)

delete\_memdump = yes (To delete memory dumps of VM)

* + - sudo nano reporting.conf

set: [mongodb] enabled = yes

report.html enabled = yes

report.pdf enabled = yes

* Reboot Ubuntu
* Starting Cuckoo
  + cuckoo community (run once in a while only)
  + vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 (Everytime after reboot)
  + cuckoo -d (in one terminal)
  + cuckoo run webserver 0.0.0.0:8000 (in another terminal)
* Open Browser, head to [0.0.0.0:8000](http://0.0.0.0:8000/) (or [127.0.0.1:8000](http://127.0.0.1:8000/)) for Web UI of Cuckoo

**Submission options:**

* Starting Cuckoo (leave this command to execute in one terminal)
  + cuckoo -d
* Single File Submission
  + cuckoo submit path/to/binary
* Bulk Submission
  + cuckoo submit --timeout 60 <path to malware binary folder>
* URL Submission
  + cuckoo submit --url [http://www.example.com](http://www.example.com/)
* Higher Priority Submission
  + cuckoo submit --priority 5 /path/to/binary
* Timeout
  + cuckoo submit --timeout 60 /path/to/binar
* Custom Time VM Submission (Format is %m-%d-%Y %H:%M:%S)
  + cuckoo submit --clock "01-24-2001 14:41:20" /path/to/binary

**Resources:**

**GitHub:** <https://github.com/ezyway/Cuckoo-Scripts>

**WindowsError: [Error 5] Access is denied:** <https://github.com/cuckoosandbox/cuckoo/issues/2150>

**Cuckoo Installation:** https://utopianknight.com/malware/cuckoo-installation-on-ubuntu-20/

**FAQ:**

1. Windows 7 (Guest) not able to access internet.
   * Check VM Network Adapter is set to Host-only Adapter and vboxnet0
   * Check IP in Windows 7(192.168.56.101 and 255.255.255 and 192.168.56.1)
   * Execute the following commands (replace ens33 with your adapter (connected to internet) name from ‘ipconfig’ command.):
     + sudo iptables -A FORWARD -o ens33 -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT
     + sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
     + sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
   * execute – sudo nano /proc/sys/net/ipv4/ip\_forward. If it is 0, set it to 1 and save the file.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated