Team Car RamRod

Project Documentation
Revision 1

An Analytic Honeypot for Virtualized Environments

Professor Andrew Bennett

Team Members:

Matthew McLeod
Patrick McDonald
Evan Leky
David Garrett May

Table of contents

Executive summary

Our team’s project was to install a honey pot and detect malware samples on a machine. The honeypot would then analyze the infected files that it was able to find. Afterwards a report of the sandbox findings would be returned to the host machine for review. We had planned on furthering the functionality of the application by allowing the sandbox to open a new session for the affected user if a live machine had been infected. Another feature that we would have liked to implement would have been the ability to establish a relationship hierarchy in order to help establish the morphology of any new samples of malware captured. Even without being able to implement these additions we have gained factual knowledge that will assist us in our professional careers.

We were able to achieve malware detection by installing an ESXi host and configuring different virtual machines to communicate through the same hypervisor in order to run Cuckoo Sandbox. Once we were able to configure Cuckoo Sandbox we were able to test the detection and result process by running the honeypot and having it check a website to ensure correct installation had taken place, in this case cnet.com was analyzed. We were then ready to deploy malware samples and Cuckoo Sandbox to detect, compare, analyze and display results. Some of the features have not been correctly configured at this time and will be fixed at a later date.

The current cost of the project and procedures are free due to the fact that we are using nothing but open source software and extended trials available to students. The main software components used for this project were Windows 7, Ubuntu, VMware Workstation, VMware vSphere, VMware ESXi, Cuckoo Sandbox. Using the listed products we were able to not only implement a honeypot using Cuckoo Sandbox but, also gain a deeper understanding of the challenges and platforms required for virtualizing a system of interdependent applications.

Scope of work

Our project was to install and configure Cuckoo Sandbox on a host machine and then attempt to modify it to aide in the discovery and logging process malware in a virtualized environment.

Project Goal

Install and configure Cuckoo Sandbox onto a host machine.

Objectives

Deliverables:

- A virtual machine that has Cuckoo Sandbox installed and configured
- Guest OS with Cuckoo client installed
- Modified version of Cuckoo Sandbox
- Website to obtain up-to-date project status and team member information

Approach:

First: we will be looking into ways to host the honeypot to allow remote access
Second: install a Sandbox environment onto a machine
Third: testing the standard installation of the Sandbox
Fourth: Modification of the Sandbox
Fifth: Testing the modified Sandbox

Timeline

June 30 - July 6: Formed group, researched topic and cloud services then presented our project proposal.
July 7-July 13: Installed ESXi on Workstation 10. Installed vSphere Client on machine and access host. Installed vSphere Client on laptop and access host. Create a virtual machine using the vSphere Client. Installed guest OS: Windows 7. Remote Access client was determined to be Team Viewer and was installed. Installed guest OS: Ubuntu (Cuckoo host)
July 9-11: Failed at everything we attempted for a couple weeks and then researched the software requirements to install and configure Cuckoo sandbox, ESXI and the required packages.
July 12-17: Received malware and attempted to understand what it was and did. Got the visual formed using Gephi.
July 18-30: Started documentation and finalized Cuckoo Sandbox installation where we could finish testing.

Milestones

Install ESXI on a remote host and access
Install Ubuntu 14.04 and Cuckoo Sandbox
Reconfigure Cuckoo Sandbox to utilize ESXI
Test Cuckoo Sandbox
Modify Cuckoo Sandbox to detect, analyze and report the malicious attacks.

Benefits

Completing this project will give our team members knowledge that will continue to help us throughout our careers in the computing sciences field. Having participated on this project we will be able to better implement security features in most networks we help implement or applications we design.

Assumptions

That the users viewing this document have basic knowledge of the operating systems Ubuntu and Windows. Also that they are familiar with the package manager in Linux. Access to VMware products or VirtualBox will be necessary to configure and run the applications.

Procedure

First VMware ESXI will need to be installed onto the host machine, see Appendix F for detailed instructions.

Then Install Ubuntu or your chosen Linux distribution into the ESXI host.

Next comes the installation of Cuckoo Sandbox, see Appendix C for the detailed instructions. Appendix D can be viewed to see the non-detailed instruction set for installation and configuration.

Install windows onto the ESXI host and after installing disable automatic updates and turn off the windows firewall.

After installing the sandbox onto the host OS the guest machine will need to have the Cuckoo agent installed so that the sandbox environment can access the machine for analysis.

Test Cuckoo box by running a simulated malware detonation.

Check for the creation of the activity report.

Closing

With the knowledge that our team gathered we were able to complete a scan of not only a website and fish for any detectable threats but also able to deploy malicious malware and have the Cuckoo Sandbox run and output the needed information to analyze the data. We gained knowledge in setting up multiple virtual machines on an ESXi host and the ability to install a difficult open-source software such as Cuckoo. We hope to have the ability in the future to further the Cuckoo experience and create the ability to analyze attacks of malware or websites on a machine allowing already encountered threats to be automatically purged without the need for analysis software to be ran.

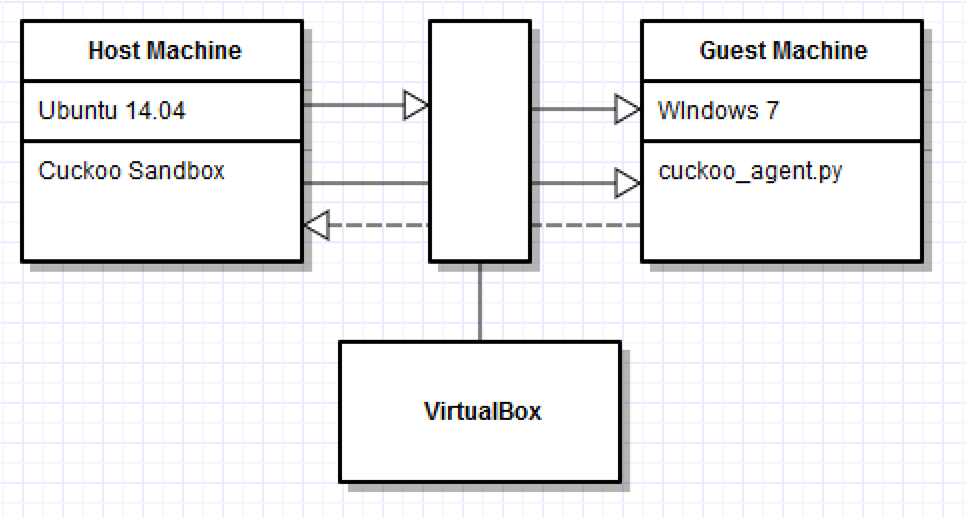
Appendix

A. Resources

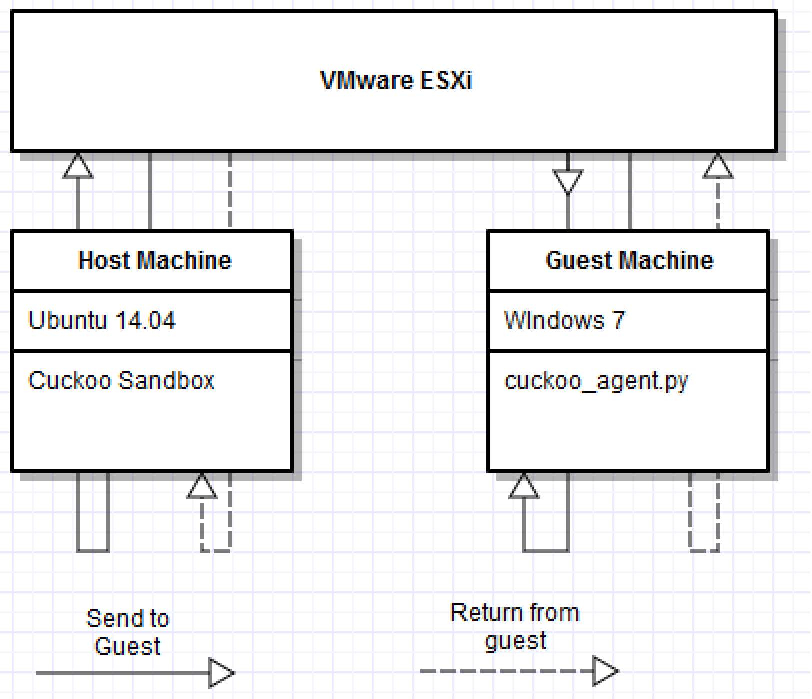
- VMware Workstation: Virtualization Environment.
- VMware vSphere: Connection Client.
- VMware vCenter: Connection Broker.
- VMware ESXI: Type one hypervisor.
- Cuckoo Sandbox: Tool that monitors virtual machines and analyses malware that is detected.
- Cuckoo Sandbox documentation
- Metasploit: a tool used to simulate malware, denial of service and other various other system exploits.
- Windows 7:
- Ubuntu 14.04:
- Gephi: application that allows the visualization of malware encountered
- http://www.nooooooooooooooo.com/ ; for our dire situations
- python 2.7 or 3.3:
- Python modules:
    - sqlalchemy
    - bson
    - dpkt
    - jinja2
    - magic
    - pydeep
    - pymongo
    - yara
    - libvirt
    - bottlepy
    - django
    - pefile
    - volatility
    - MAEC Python bindings
    - Chardet
    - tcpdump

B. Diagrams

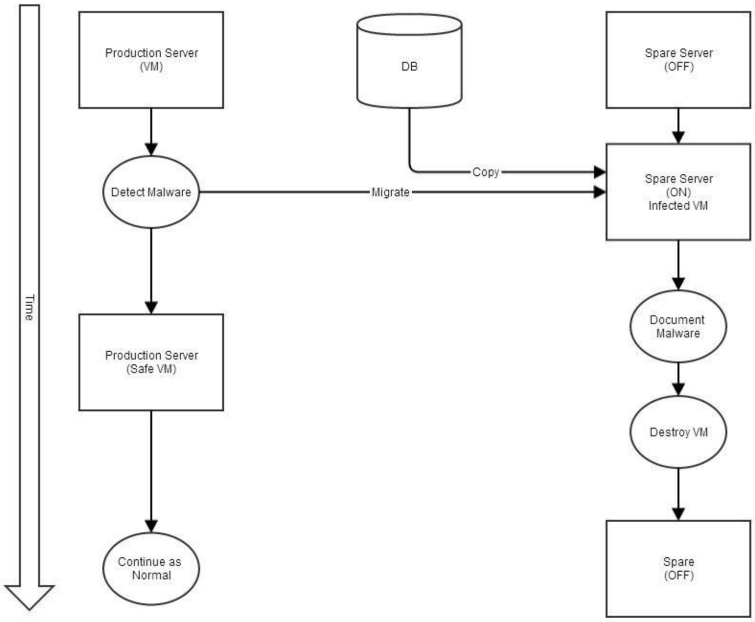
Standard Cuckoo Sandbox Configuration



Project Cuckoo Sandbox Setup



Proposed Setup of finished project



C. Installation Process for CuckooBox

For a shortened version of these instructions see Appendix D.

Installing CuckooBox requires that python and several of its third party libraries are installed to function properly. As such getting CuckooBox to run is an undertaking that requires for several steps to be followed to ensure the application will run properly. Also needed is a virtualized environment such as VirtualBox or VMware workstation. For this project we used “”, its installation will be covered in Appendix “”. Many of these packages will need to be installed at the root level in order to function properly so the use of the “sudo” terminal command prefix will be prevalent during this install.

First off the host machine will require python, in Linux you can check for its installation by typing python into the terminal and pressing return. If python is installed the blinking cursor will be preceded by “>>>”, to exit type quit() and press return. If python is not present you will likely get and error and a prompt explaining how to download python via the terminal package manager if one is present. In a debian distribution of Linux (Ubuntu or Debian) the terminal command below will fetch the files and install them automatically. During this process you may be prompted to enter the admin password and confirm that you would like to download the files.

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

Once python is installed on the system, the user is advised to install pip a package manager for python. This makes installing most of the needed packages for Python a much easier process by allowing the download and installation process to be automated. This can be done via the command below. While this step is optional it is the preferred method for installing most python packages regardless of operating system.

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

After installing pip the next group of files to install are the sqlalchemy and bson packages for python as well. Below are the commands for installing them with or without pip.

With pip: sudo pip install sqlalchemy bson

Without pip: sudo apt-get install python-sqlalchemy python-bson

Next the majority of the remaining python libraries can be installed by a single pip or apt-get call in the terminal. If for some reason the command fails to install all of the plugins at once they can be entered individually. Pip will not be able to install all of these libraries so the debian repository is recommended for this step to ease the installation.

with pip: sudo pip install jinja2 pymongo bottle pefile maec==4.0.1.0 django chardet

without pip: sudo apt-get install python-dpkt python-jinja2 python-magic python-pymongo python-gridfs python-libvirt python-bottle python-pefile python-chardet

After installing the above libraries Tcpdump will need to be installed onto the host in order for Cuckoo to log the network traffic of the guest operating systems in the honeypot environment. This can be achieved via the apt-get command below

```
sudo apt-get install tcpdump
```

After downloading this package it is best to configure and set it up immediately in order to avoid problems later in the installation process. elow are the commands to configure tcpdump. If you do not have the package libcap2-bin install it first or the setcap command will fail.

If libcap2-bin not present:

```
sudo apt-get install libcap2-bin
```

Giving root privileges to tcpdump and allow Cuckoo to access it:

```
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

To check that the last command was successful:

```
getcap /usr/sbin/tcpdump
```

The result should be: /usr/sbin/tcpdump = cap_net_admin, cap_net_raw+eip

Before installing the Cuckoo files if the person installing the software wishes they may create a new user specifically for the application. This can be done by the command below.

```
sudo adduser cuckoo
```

Then if you will need to ad access to the virtualization software for the new user, via the command below. The portion in the <> braces will be the user group for the virtualization software that is being utilized.

```
sudo usermod -G <virtualization software users> cuckoo
```

Lastly before installing Cuckoo box the cuckoo user must be added into the libvirtd package group.

```
sudo usermod -G libvirtd cuckoo
```

After following all of the above steps the system is now ready to have CuckooBox installed and configured. If you do not have the git package downloaded it can be installed by the apt-get command below. If git is already installed you can clone the cuckoo repository with the second command below

```
sudo apt-get install git
 git clone git://github.com/cuckoobox.git
```

After this step cuckoo is installed but will now need to be configured. Cuckoo.conf is the first file that needs to be altered. it has most of the generic settings for Cuckoo and is well commented so that most of the setting.

Auxilary.conf is the file that will determine whether or not the optional module tcpdump will be utilized. It also tells CuckooBox where to find the package and what networks tcpdump should be monitoring.

<machinery>.conf are the files that contain the instructions of which VMs cuckoo box should interact with and how it should do so. In these files you will need to specify the display mode, path to the virtualization software, a list of the available machines to be used, their labels, operating systems, IP address of the current virtual machine, snapshot, NIC, IP of the result server, port of the result server, and whatever tags you would like for the machines.

Before enabling memory.conf to use Volatility two config files must be present and tuned. Processing.conf and memory_dump in cuckoo.conf

memory.conf is where the volatility tool profiles will be configured for memory dump operations. Each of the profiles will be controlled by the volatility.conf file. You can also select if you would like to keep the memory dumps after they have been processed.

D. Simplified Cuckoo Installation notes

```
sudo apt-get install python
sudo apt-get install python-pip
sudo apt-get install python-sqlalchemy python-bson
sudo apt-get install python-dpkt python-jinja2 python-magic
        python-pymongo python-gridfs python-libvirt
        python-bottle python-pefile python-chardet
sudo apt-get install libcap2-bin
sudo apt-get install tcpdump
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
getcap /usr/sbin/tcpdump
sudo adduser cuckoo
sudo usermod -G <virtualization software users> cuckoo
sudo usermod -G libvirtd cuckoo
sudo apt-get install git
git clone git://github.com/cuckoobox.git
```

Followed by file configuration on host and guest

E. Expected screen output during installation of Cuckoo Sandbox

```
tester@ubuntu:~$ python
Python 2.7.6 (default, Mar 22 2014, 22:59:56)
[GCC 4.8.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> quit()

tester@ubuntu:~$ sudo apt-get install python-sqlalchemy pthon-bson
[sudo] password for tester:
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package pthon-bson

tester@ubuntu:~$ sudo apt-get install python-sqlalchemy python-bson
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
python-bson-ext python-sqlalchemy-ext
Suggested packages:
python-sqlalchemy-doc python-psycopg2 python-mysqldb python-kinterbasdb
python-pymssql
```

```
The following NEW packages will be installed:
python-bson python-bson-ext python-sqlalchemy python-sqlalchemy-ext
0 upgraded, 4 newly installed, 0 to remove and 322 not upgraded.
Need to get 581 kB of archives.
After this operation, 3,534 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-bson amd64 2.6.3-1build1 [18.4 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-bson-ext amd64 2.6.3-1build1 [17.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-sqlalchemy all 0.8.4-1build1 [532 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-sqlalchemy-ext amd64 0.8.4-1build1 [13.6 kB]
Fetched 581 kB in 1s (474 kB/s)
Selecting previously unselected package python-bson.
(Reading database ... 163348 files and directories currently installed.)
Preparing to unpack .../python-bson_2.6.3-1build1_amd64.deb …
Unpacking python-bson (2.6.3-1build1) …
Selecting previously unselected package python-bson-ext.
Preparing to unpack .../python-bson-ext_2.6.3-1build1_amd64.deb …
Unpacking python-bson-ext (2.6.3-1build1) …
Selecting previously unselected package python-sqlalchemy.
Preparing to unpack .../python-sqlalchemy_0.8.4-1build1_all.deb …
Unpacking python-sqlalchemy (0.8.4-1build1) …
Selecting previously unselected package python-sqlalchemy-ext.
Preparing to unpack .../python-sqlalchemy-ext_0.8.4-1build1_amd64.deb …
Unpacking python-sqlalchemy-ext (0.8.4-1build1) ...
Setting up python-bson (2.6.3-1build1) ...
Setting up python-bson-ext (2.6.3-1build1) ...
Setting up python-sqlalchemy (0.8.4-1build1) ...
Setting up python-sqlalchemy-ext (0.8.4-1build1) ...

tester@ubuntu:~$ sudo apt-get install python-dpkt python-jinja2 python-magic python-pymongo python-gridfs python-libvirt python-bottle python-pefile python-chardet
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-chardet is already the newest version.
The following extra packages will be installed:
  augeas-lenses bridge-utils cgroup-lite ebtables file gawk libaugeas0
  libboost-thread1.54.0 libmagic1 libnetcf1 librados2 librbd1 libsigsegv2
  libvirt-bin libvirt0 libxen-4.4 libxenstore3.0 libxml2-utils python-markupsafe
  python-pymongo-ext python-support
```

```
Suggested packages:
  augeas-doc gawk-doc augeas-tools qemu-kvm qemu radvd lvm2 python-jinja2-doc
The following NEW packages will be installed:
  augeas-lenses bridge-utils cgroup-lite ebtables gawk libaugeas0
  libboost-thread1.54.0 libnetcf1 librados2 librbd1 libsigsegv2 libvirt-bin
  libvirt0 libxen-4.4 libxenstore3.0 libxml2-utils python-bottle python-dpkt
  python-gridfs python-jinja2 python-libvirt python-magic python-markupsafe
  python-pefile python-pymongo python-pymongo-ext python-support
The following packages will be upgraded:
  file libmagic1
2 upgraded, 27 newly installed, 0 to remove and 320 not upgraded.
Need to get 7,031 kB of archives.
After this operation, 32.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main file amd64 1:5.14-
2ubuntu3.1 [18.8 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libmagic1 amd64 1:5.14-
2ubuntu3.1 [184 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty/main libsigsegv2 amd64 2.10-2 [15.0
kB]
Get:4 http://us.archive.ubuntu.com/ubuntu/ trusty/main gawk amd64 1:4.0.1+dfsg-
2.1ubuntu2 [781 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libboost-thread1.54.0
amd64 1.54.0-4ubuntu3.1 [26.5 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main librados2 amd64 0.80.1-
0ubuntu1.1 [1,408 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main librbd1 amd64 0.80.1-
0ubuntu1.1 [316 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu/ trusty/main augeas-lenses all 1.2.0-0ubuntu1
[229 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu/ trusty/main bridge-utils amd64 1.5-6ubuntu2
[29.2 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu/ trusty/main ebtables amd64 2.0.10.4-
3ubuntu1 [77.5 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu/ trusty/main libaugeas0 amd64 1.2.0-
0ubuntu1 [140 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu/ trusty/main libnetcf1 amd64 1:0.2.3-
4ubuntu1 [44.4 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libvirt0 amd64 1.2.2-
0ubuntu13.1.1 [832 kB]
Get:14 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libxenstore3.0 amd64
4.4.0-0ubuntu5.1 [18.5 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libxen-4.4 amd64
4.4.0-0ubuntu5.1 [272 kB]
```

```
Get:16 http://us.archive.ubuntu.com/ubuntu/ trusty/main cgroup-lite all 1.9 [3,918 B]
Get:17 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libvirt-bin amd64 1.2.2-0ubuntu13.1.1 [2,063 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libxml2-utils amd64 2.9.1+dfsg1-3ubuntu4.3 [34.7 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu/ trusty/universe python-bottle all 0.12.0-1 [40.1 kB]
Get:20 http://us.archive.ubuntu.com/ubuntu/ trusty/universe python-support all 1.0.15 [26.7 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu/ trusty/universe python-dpkt all 1.6+svn54-1 [62.2 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-pymongo amd64 2.6.3-1build1 [73.7 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-gridfs all 2.6.3-1build1 [10.2 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-markupsafe amd64 0.18-1build2 [14.3 kB]
Get:25 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-jinja2 all 2.7.2-2 [161 kB]
Get:26 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-libvirt amd64 1.2.2-0ubuntu1 [97.6 kB]
Get:27 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-pymongo-ext amd64 2.6.3-1build1 [8,960 B]
Get:28 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/universe python-magic all 1:5.14-2ubuntu3.1 [4,514 B]
Get:29 http://us.archive.ubuntu.com/ubuntu/ trusty/universe python-pefile all 1.2.9.1-1.1 [37.8 kB]
Fetched 7,031 kB in 5s (1,276 kB/s)
(Reading database ... 163567 files and directories currently installed.)
Preparing to unpack .../file_1%3a5.14-2ubuntu3.1_amd64.deb ...
Unpacking file (1:5.14-2ubuntu3.1) over (1:5.14-2ubuntu3) ...
Preparing to unpack .../libmagic1_1%3a5.14-2ubuntu3.1_amd64.deb ...
Unpacking libmagic1:amd64 (1:5.14-2ubuntu3.1) over (1:5.14-2ubuntu3) ...
Selecting previously unselected package libsigsegv2:amd64.
Preparing to unpack .../libsigsegv2_2.10-2_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.10-2) ...
Processing triggers for man-db (2.6.7.1-1) ...
/usr/bin/mandb: warning: can't update index cache /var/cache/man/index.db: Resource temporarily unavailable
Setting up libsigsegv2:amd64 (2.10-2) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Selecting previously unselected package gawk.
(Reading database ... 163575 files and directories currently installed.)
Preparing to unpack .../gawk_1%3a4.0.1+dfsg-2.1ubuntu2_amd64.deb ...
Unpacking gawk (1:4.0.1+dfsg-2.1ubuntu2) ...
```

```
Selecting previously unselected package libboost-thread1.54.0:amd64.
Preparing to unpack .../libboost-thread1.54.0_1.54.0-4ubuntu3.1_amd64.deb ...
Unpacking libboost-thread1.54.0:amd64 (1.54.0-4ubuntu3.1) ...
Selecting previously unselected package librados2.
Preparing to unpack .../librados2_0.80.1-0ubuntu1.1_amd64.deb ...
Unpacking librados2 (0.80.1-0ubuntu1.1) ...
Selecting previously unselected package librbd1.
Preparing to unpack .../librbd1_0.80.1-0ubuntu1.1_amd64.deb ...
Unpacking librbd1 (0.80.1-0ubuntu1.1) ...
Selecting previously unselected package augeas-lenses.
Preparing to unpack .../augeas-lenses_1.2.0-0ubuntu1_all.deb ...
Unpacking augeas-lenses (1.2.0-0ubuntu1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../bridge-utils_1.5-6ubuntu2_amd64.deb ...
Unpacking bridge-utils (1.5-6ubuntu2) ...
Selecting previously unselected package ebtables.
Preparing to unpack .../ebtables_2.0.10.4-3ubuntu1_amd64.deb ...
Unpacking ebtables (2.0.10.4-3ubuntu1) ...
Selecting previously unselected package libaugeas0.
Preparing to unpack .../libaugeas0_1.2.0-0ubuntu1_amd64.deb ...
Unpacking libaugeas0 (1.2.0-0ubuntu1) ...
Selecting previously unselected package libnetcf1.
Preparing to unpack .../libnetcf1_1%3a0.2.3-4ubuntu1_amd64.deb ...
Unpacking libnetcf1 (1:0.2.3-4ubuntu1) ...
Selecting previously unselected package libvirt0.
Preparing to unpack .../libvirt0_1.2.2-0ubuntu13.1.1_amd64.deb ...
Unpacking libvirt0 (1.2.2-0ubuntu13.1.1) ...
Selecting previously unselected package libxenstore3.0.
Preparing to unpack .../libxenstore3.0_4.4.0-0ubuntu5.1_amd64.deb ...
Unpacking libxenstore3.0 (4.4.0-0ubuntu5.1) ...
Selecting previously unselected package libxen-4.4.
Preparing to unpack .../libxen-4.4_4.4.0-0ubuntu5.1_amd64.deb ...
Unpacking libxen-4.4 (4.4.0-0ubuntu5.1) ...
Selecting previously unselected package cgroup-lite.
Preparing to unpack .../cgroup-lite_1.9_all.deb ...
Unpacking cgroup-lite (1.9) ...
Selecting previously unselected package libvirt-bin.
Preparing to unpack .../libvirt-bin_1.2.2-0ubuntu13.1.1_amd64.deb ...
Unpacking libvirt-bin (1.2.2-0ubuntu13.1.1) ...
Selecting previously unselected package libxml2-utils.
Preparing to unpack .../libxml2-utils_2.9.1+dfsg1-3ubuntu4.3_amd64.deb ...
Unpacking libxml2-utils (2.9.1+dfsg1-3ubuntu4.3) ...
Selecting previously unselected package python-bottle.
Preparing to unpack .../python-bottle_0.12.0-1_all.deb ...
```

```
Unpacking python-bottle (0.12.0-1) ...
Selecting previously unselected package python-support.
Preparing to unpack .../python-support_1.0.15_all.deb ...
Unpacking python-support (1.0.15) ...
Selecting previously unselected package python-dpkt.
Preparing to unpack .../python-dpkt_1.6+svn54-1_all.deb ...
Unpacking python-dpkt (1.6+svn54-1) ...
Selecting previously unselected package python-pymongo.
Preparing to unpack .../python-pymongo_2.6.3-1build1_amd64.deb ...
Unpacking python-pymongo (2.6.3-1build1) ...
Selecting previously unselected package python-gridfs.
Preparing to unpack .../python-gridfs_2.6.3-1build1_all.deb ...
Unpacking python-gridfs (2.6.3-1build1) ...
Selecting previously unselected package python-markupsafe.
Preparing to unpack .../python-markupsafe_0.18-1build2_amd64.deb ...
Unpacking python-markupsafe (0.18-1build2) ...
Selecting previously unselected package python-jinja2.
Preparing to unpack .../python-jinja2_2.7.2-2_all.deb ...
Unpacking python-jinja2 (2.7.2-2) ...
Selecting previously unselected package python-libvirt.
Preparing to unpack .../python-libvirt_1.2.2-0ubuntu1_amd64.deb ...
Unpacking python-libvirt (1.2.2-0ubuntu1) ...
Selecting previously unselected package python-pymongo-ext.
Preparing to unpack .../python-pymongo-ext_2.6.3-1build1_amd64.deb ...
Unpacking python-pymongo-ext (2.6.3-1build1) ...
Selecting previously unselected package python-magic.
Preparing to unpack .../python-magic_1%3a5.14-2ubuntu3.1_all.deb ...
Unpacking python-magic (1:5.14-2ubuntu3.1) ...
Selecting previously unselected package python-pefile.
Preparing to unpack .../python-pefile_1.2.9.1-1.1_all.deb ...
Unpacking python-pefile (1.2.9.1-1.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up libmagic1:amd64 (1:5.14-2ubuntu3.1) ...
Setting up file (1:5.14-2ubuntu3.1) ...
Setting up gawk (1:4.0.1+dfsg-2.1ubuntu2) ...
Setting up libboost-thread1.54.0:amd64 (1.54.0-4ubuntu3.1) ...
Setting up librados2 (0.80.1-0ubuntu1.1) ...
Setting up librbd1 (0.80.1-0ubuntu1.1) ...
Setting up augeas-lenses (1.2.0-0ubuntu1) ...
Setting up bridge-utils (1.5-6ubuntu2) ...
Setting up ebtables (2.0.10.4-3ubuntu1) ...
Setting up libaugeas0 (1.2.0-0ubuntu1) ...
Setting up libnetcf1 (1:0.2.3-4ubuntu1) ...
Setting up libvirt0 (1.2.2-0ubuntu13.1.1) ...
Setting up libxenstore3.0 (4.4.0-0ubuntu5.1) ...
Setting up libxen-4.4 (4.4.0-0ubuntu5.1) ...
Setting up cgroup-lite (1.9) ...
cgroup-lite start/running
Setting up libxml2-utils (2.9.1+dfsg1-3ubuntu4.3) ...
Setting up python-bottle (0.12.0-1) ...
Setting up python-support (1.0.15) ...
Setting up python-dpkt (1.6+svn54-1) ...
Setting up python-pymongo (2.6.3-1build1) ...
Setting up python-gridfs (2.6.3-1build1) ...
Setting up python-markupsafe (0.18-1build2) ...
Setting up python-jinja2 (2.7.2-2) ...
Setting up python-libvirt (1.2.2-0ubuntu1) ...
Setting up python-pymongo-ext (2.6.3-1build1) ...
Setting up python-magic (1:5.14-2ubuntu3.1) ...
Setting up python-pefile (1.2.9.1-1.1) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up libvirt-bin (1.2.2-0ubuntu13.1.1) ...
Adding group `libvirtd' (GID 125) ...
Done.
libvirt-bin start/running, process 11846
Setting up libvirt-bin dnsmasq configuration.
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for python-support (1.0.15) ...
Processing triggers for ureadahead (0.100.0-16) ...

tester@ubuntu:~$ sudo apt-get install dkms
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  fakeroot libfakeroot
Suggested packages:
  dpkg-dev debhelper
The following NEW packages will be installed:
  dkms fakeroot libfakeroot
0 upgraded, 3 newly installed, 0 to remove and 320 not upgraded.
Need to get 145 kB of archives.
After this operation, 764 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main dkms all 2.2.0.3-1.1ubuntu5 [64.4
kB]
```

```
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty/main libfakeroot amd64 1.20-3ubuntu2
[25.4 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty/main fakeroot amd64 1.20-3ubuntu2
[55.0 kB]
Fetched 145 kB in 0s (247 kB/s)
Selecting previously unselected package dkms.
(Reading database ... 164603 files and directories currently installed.)
Preparing to unpack .../dkms_2.2.0.3-1.1ubuntu5_all.deb ...
Unpacking dkms (2.2.0.3-1.1ubuntu5) ...
Selecting previously unselected package libfakeroot:amd64.
Preparing to unpack .../libfakeroot_1.20-3ubuntu2_amd64.deb ...
Unpacking libfakeroot:amd64 (1.20-3ubuntu2) ...
Selecting previously unselected package fakeroot.
Preparing to unpack .../fakeroot_1.20-3ubuntu2_amd64.deb ...
Unpacking fakeroot (1.20-3ubuntu2) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up dkms (2.2.0.3-1.1ubuntu5) ...
Setting up libfakeroot:amd64 (1.20-3ubuntu2) ...
Setting up fakeroot (1.20-3ubuntu2) ...
update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in
auto mode

tester@ubuntu:~$ sudo dpkg -i VirtualBox-4.3_4.3.14_Ubuntu_raring_i386.deb
dpkg: error processing archive VirtualBox-4.3_4.3.14_Ubuntu_raring_i386.deb (--install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 VirtualBox-4.3_4.3.14_Ubuntu_raring_i386.deb

tester@ubuntu:~$ sudo dpkg -i VirtualBox-4.3_4.3.14~Ubuntu~raring_amd64.deb
dpkg: error processing archive VirtualBox-4.3_4.3.14~Ubuntu~raring_amd64.deb (--
install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 VirtualBox-4.3_4.3.14~Ubuntu~raring_amd64.deb

tester@ubuntu:~$ sudo dpkg -i VirtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb
dpkg: error processing archive VirtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb (--
install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 VirtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb
tester@ubuntu:~$ ls
Desktop    Downloads         Music     Public  Videos
Documents  examples.desktop  Pictures  Templates
```

```
tester@ubuntu:~$ cd downloads
bash: cd: downloads: No such file or directory

tester@ubuntu:~$ cd Downloads

tester@ubuntu:~/Downloads$ sudo dpkg -i VirtualBox-
4.3_4.3.14_Ubuntu_raring_amd64.debdpkg: error processing archive VirtualBox-
4.3_4.3.14_Ubuntu_raring_amd64.deb (--install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 VirtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb
tester@ubuntu:~/Downloads$ dir
virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb

tester@ubuntu:~/Downloads$ sudo dpkg -i VirtualBox-
4.3_4.3.14_Ubuntu_raring_amd64.debdpkg: error processing archive VirtualBox-
4.3_4.3.14_Ubuntu_raring_amd64.deb (--install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 VirtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb

tester@ubuntu:~/Downloads$ dir
virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb

tester@ubuntu:~/Downloads$ sudo dpkg -i virtualBox-
4.3_4.3.14_Ubuntu_raring_amd64.deb
dpkg: error processing archive virtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb (--
install):
 cannot access archive: No such file or directory
Errors were encountered while processing:
 virtualBox-4.3_4.3.14_Ubuntu_raring_amd64.deb

tester@ubuntu:~/Downloads$ sudo /etc/init.d/vboxdrv setup
sudo: /etc/init.d/vboxdrv: command not found

tester@ubuntu:~/Downloads$ ./VirtualBox.run --keep --noexec
bash: ./VirtualBox.run: No such file or directory

tester@ubuntu:~/Downloads$ dir
virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb

tester@ubuntu:~/Downloads$ cd .
tester@ubuntu:~/Downloads$ ls
```

```
virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb

tester@ubuntu:~/Downloads$ sudo dpkg virtualbox-4.3_4.3.14-
95030~Ubuntu~raring_amd64.deb
dpkg: error: need an action option

Type dpkg --help for help about installing and deinstalling packages [*];
Use 'apt' or 'aptitude' for user-friendly package management;
Type dpkg -Dhelp for a list of dpkg debug flag values;
Type dpkg --force-help for a list of forcing options;
Type dpkg-deb --help for help about manipulating *.deb files;

Options marked [*] produce a lot of output - pipe it through 'less' or 'more' !

tester@ubuntu:~/Downloads$ sudo dpkg -i virtualbox-4.3_4.3.14-
95030~Ubuntu~raring_amd64.deb
Selecting previously unselected package virtualbox-4.3.
(Reading database ... 164694 files and directories currently installed.)
Preparing to unpack virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb ...
Unpacking virtualbox-4.3 (4.3.14-95030~Ubuntu~raring) ...
dpkg: dependency problems prevent configuration of virtualbox-4.3:
 virtualbox-4.3 depends on libsdl1.2debian (>= 1.2.11); however:
  Package libsdl1.2debian is not installed.

dpkg: error processing package virtualbox-4.3 (--install):
 dependency problems - leaving unconfigured
Processing triggers for ureadahead (0.100.0-16) ...
Processing triggers for shared-mime-info (1.2-0ubuntu3) ...
Processing triggers for gnome-menus (3.10.1-0ubuntu2) ...
Processing triggers for desktop-file-utils (0.22-1ubuntu1) ...
Processing triggers for bamfdaemon (0.5.1+14.04.20140409-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.54ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.13-1) ...
Errors were encountered while processing:
 virtualbox-4.3

tester@ubuntu:~/Downloads$ sudo apt-get install VirtualBox
Reading package lists... Done
Building dependency tree
Reading state information... Done
You might want to run 'apt-get -f install' to correct these:
The following packages have unmet dependencies:
 virtualbox : Depends: libgsoap4 but it is not going to be installed
```

```
            Depends: libsdl1.2debian (>= 1.2.11) but it is not going to be installed
            Recommends: virtualbox-dkms (= 4.3.10-dfsg-1) but it is not going to be installed
or
                        virtualbox-source (= 4.3.10-dfsg-1) but it is not going to be installed
            Recommends: virtualbox-qt (= 4.3.10-dfsg-1) but it is not going to be installed
 virtualbox-4.3 : Depends: libsdl1.2debian (>= 1.2.11) but it is not going to be installed
                        Recommends: libsdl-ttf2.0-0 but it is not going to be installed
                        Conflicts: virtualbox
E: Unmet dependencies. Try 'apt-get -f install' with no packages (or specify a solution).
tester@ubuntu:~/Downloads$ sudo apt-get install libgsoap4
Reading package lists... Done
Building dependency tree
Reading state information... Done
You might want to run 'apt-get -f install' to correct these:
The following packages have unmet dependencies:
 virtualbox-4.3 : Depends: libsdl1.2debian (>= 1.2.11) but it is not going to be installed
                        Recommends: libsdl-ttf2.0-0 but it is not going to be installed
E: Unmet dependencies. Try 'apt-get -f install' with no packages (or specify a solution).

tester@ubuntu:~/Downloads$ sudo apt-get -f  install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following extra packages will be installed:
  libsdl1.2debian
The following NEW packages will be installed:
  libsdl1.2debian
0 upgraded, 1 newly installed, 0 to remove and 320 not upgraded.
1 not fully installed or removed.
Need to get 162 kB of archives.
After this operation, 496 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libsdl1.2debian amd64
1.2.15-8ubuntu1.1 [162 kB]
Fetched 162 kB in 0s (285 kB/s)
Selecting previously unselected package libsdl1.2debian:amd64.
(Reading database ... 165441 files and directories currently installed.)
Preparing to unpack .../libsdl1.2debian_1.2.15-8ubuntu1.1_amd64.deb ...
Unpacking libsdl1.2debian:amd64 (1.2.15-8ubuntu1.1) ...
Setting up libsdl1.2debian:amd64 (1.2.15-8ubuntu1.1) ...
Setting up virtualbox-4.3 (4.3.14-95030~Ubuntu~raring) ...
Adding group `vboxusers' (GID 127) ...
Done.
```

```
Stopping VirtualBox kernel modules ...done.
Uninstalling old VirtualBox DKMS kernel modules ...done.
Trying to register the VirtualBox kernel modules using DKMS ...done.
Starting VirtualBox kernel modules ...done.
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for ureadahead (0.100.0-16) ...

tester@ubuntu:~/Downloads$ sudo apt-get install tcpdump
[sudo] password for tester:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 320 not upgraded.
tester@ubuntu:~/Downloads$ sudo setcap cap_net_raw,cap_net_admin=eip
/usr/sbin/tcpdump
tester@ubuntu:~/Downloads$ getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip

tester@ubuntu:~/Downloads$ 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' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for cuckoo
Enter the new value, or press ENTER for the default
   Full Name []: cuckoo
   Room Number []: 00
```

```
    Work Phone []: 000000000
    Home Phone []: 000000000
    Other []: 0000000000
Is the information correct? [Y/n] y

tester@ubuntu:~/Downloads$ sudo usermod -G vboxusers cuckoo

tester@ubuntu:~/Downloads$ sudo usermod -G libvirtd cuckoo

tester@ubuntu:~/Downloads$ git clone git://github.com/cuckoobox/cuckoo.git
The program 'git' is currently not installed. You can install it by typing:
sudo apt-get install git

tester@ubuntu:~/Downloads$ sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb
  git-arch git-bzr git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 320 not upgraded.
Need to get 3,274 kB of archives.
After this operation, 21.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main liberror-perl all 0.17-1.1 [21.1 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty/main git-man all 1:1.9.1-1 [698 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty/main git amd64 1:1.9.1-1 [2,555 kB]
Fetched 3,274 kB in 2s (1,332 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 165451 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17-1.1_all.deb ...
Unpacking liberror-perl (0.17-1.1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a1.9.1-1_all.deb ...
Unpacking git-man (1:1.9.1-1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a1.9.1-1_amd64.deb ...
4Unpacking git (1:1.9.1-1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up liberror-perl (0.17-1.1) ...
Setting up git-man (1:1.9.1-1) ...
Setting up git (1:1.9.1-1) ...
tester@ubuntu:~/Downloads$ git clone git://github.com/cuckoobox/cuckoo.git
Cloning into 'cuckoo'...
remote: Reusing existing pack: 18020, done.
remote: Counting objects: 172, done.
remote: Compressing objects: 100% (168/168), done.
remote: Total 18192 (delta 96), reused 0 (delta 0)
Receiving objects: 100% (18192/18192), 10.01 MiB | 873.00 KiB/s, done.
Resolving deltas: 100% (8197/8197), done.
Checking connectivity... done.
tester@ubuntu:~/Downloads$ ls
cuckoo  virtualbox-4.3_4.3.14-95030~Ubuntu~raring_amd64.deb
tester@ubuntu:~/Downloads$ cd cuckoo
tester@ubuntu:~/Downloads/cuckoo$ ls
agent     conf       data  lib      README.md         tests  web
analyzer  cuckoo.py  docs  modules  requirements.txt  utils

tester@ubuntu:~/Downloads/cuckoo$
```

F. Installing ESXI

The first steps in installing the ESXi server is to download the VMWare ESXi software and once you start you will launch the ESXi Installer. Server configuration will be displayed as the installer loads all the necessary modules. You then install the ESXi in the following screen and accept the VMware EULA by pressing F11. You then decide which disk to install the ESXi on from the list of disk groups the installer will display. Once the ESXi is confirmed the actual installation progress will begin. Once you have successfully completed the installation you will receive a prompt to reboot the server and then have the ability to configure the system.

G. Reports

Cuckoo Sandbox scan of URL: www.cnet.com

analysis.log

```
2014-07-29 12:31:56,015 [root] INFO: Starting analyzer from: C:\arlsn
2014-07-29 12:31:56,015 [root] INFO: Storing results at: C:\rVwihHR
2014-07-29 12:31:56,015 [root] INFO: Pipe server name: \\.\PIPE\uyrTdD
2014-07-29 12:31:56,015 [root] INFO: No analysis package specified, trying to detect it
        automagically.
2014-07-29 12:31:56,015 [root] INFO: Automatically selected analysis package "ie"
2014-07-29 12:32:00,086 [root] INFO: Started auxiliary module Disguise
2014-07-29 12:32:00,101 [root] INFO: Started auxiliary module Human
2014-07-29 12:32:00,118 [root] INFO: Started auxiliary module Screenshots
2014-07-29 12:32:00,211 [lib.api.process] INFO: Successfully executed process from
        path "C:\Program Files\Internet Explorer\iexplore.exe" with arguments
        ""http://www.cnet.com"" with pid 2004
2014-07-29 12:32:00,289 [lib.api.process] INFO: Using QueueUserAPC injection.
2014-07-29 12:32:00,289 [lib.api.process] INFO: Successfully injected process with
        pid 2004.
2014-07-29 12:32:02,395 [lib.api.process] INFO: Successfully resumed process with
        pid 2004
2014-07-29 12:32:02,691 [root] INFO: Added new process to list with pid: 2004
```

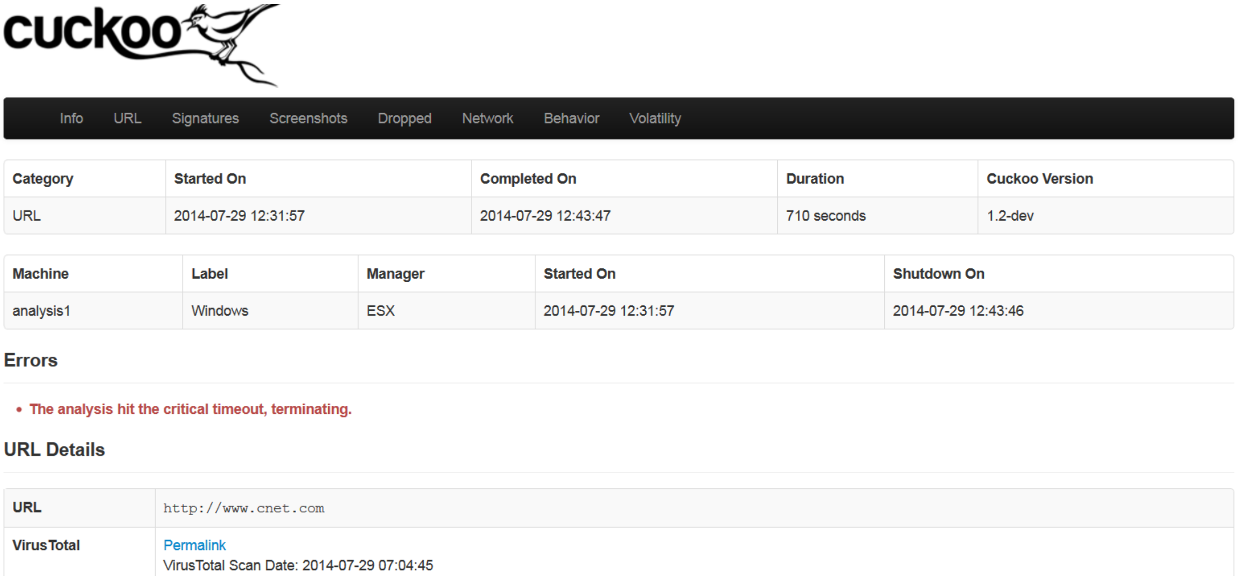
report.json

```
{
        "info": {
        "category": "url",
        "package": "",
        "started": "2014-07-29 12:31:57",
        "custom": "",
        "machine": {
        "shutdown_on": "2014-07-29 12:43:46",
        "label": "Windows",
        "manager": "ESX",
        "started_on": "2014-07-29 12:31:57",
        "id": 1,
        "name": "analysis1"
        },
        "ended": "2014-07-29 12:43:47",
        "version": "1.2-dev",
        "duration": 710,
        "id": 1
        },
        "signatures": [],
        "static": {},
        "dropped": [],
        "behavior": {
        "processtree": [],
        "processes": [],
        "anomaly": [],
        "enhanced": [],
        "summary": {
        "files": [],
        "keys": [],
        "mutexes": []
        }
        },
        "target": {
        "category": "url",
        "url": "http://www.cnet.com"
        },
        "debug": {
        "errors": [
        "The analysis hit the critical timeout, terminating."
        ],
        "log": "2014-07-29 12:31:56,015 [root] INFO: Starting analyzer from:
C:\\arlsn\n2014-07-29 12:31:56,015 [root] INFO: Storing results at: C:\\rVwihHR\n2014-
07-29 12:31:56,015 [root] INFO: Pipe server name: \\\\.\\PIPE\\uyrTdD\n2014-07-29
12:31:56,015 [root] INFO: No analysis package specified, trying to detect it
automagically.\n2014-07-29 12:31:56,015 [root] INFO: Automatically selected analysis
package \"ie\"\n2014-07-29 12:32:00,086 [root] INFO: Started auxiliary module
Disguise\n2014-07-29 12:32:00,101 [root] INFO: Started auxiliary module
Human\n2014-07-29 12:32:00,118 [root] INFO: Started auxiliary module
Screenshots\n2014-07-29 12:32:00,211 [lib.api.process] INFO: Successfully executed
process from path \"C:\\Program Files\\Internet Explorer\\iexplore.exe\" with arguments
\"\"http://www.cnet.com\"\" with pid 2004\n2014-07-29 12:32:00,289 [lib.api.process]
INFO: Using QueueUserAPC injection.\n2014-07-29 12:32:00,289 [lib.api.process]
INFO: Successfully injected process with pid 2004.\n2014-07-29 12:32:02,395
[lib.api.process] INFO: Successfully resumed process with pid 2004\n2014-07-29
12:32:02,691 [root] INFO: Added new process to list with pid: 2004\n"
        },
        "strings": [],
        "virustotal": {
        "permalink":
"https://www.virustotal.com/url/99bee484f1322e460b9b56bfdef5c60cc155c2e88a18fbcc
5589daedba36c4c8/analysis/1406617485/",
    "url": "http://www.cnet.com/",
    "response_code": 1,
    "scan_date": "2014-07-29 07:04:45",
    "scan_id":
"99bee484f1322e460b9b56bfdef5c60cc155c2e88a18fbcc5589daedba36c4c8-
1406617485",
    "verbose_msg": "Scan finished, scan information embedded in this object",
    "filescan_id": null,
    "positives": 0,
    "total": 57,
    "scans": {
    "CLEAN MX": {
        "detected": false,
        "result": "clean site"
    },
    "MalwarePatrol": {
        "detected": false,
        "result": "clean site"
    },
    "ZDB Zeus": {
        "detected": false,
        "result": "clean site"
    },
    "Tencent": {
        "detected": false,
        "result": "clean site"
    },
    "AutoShun": {
        "detected": false,
        "result": "unrated site"
    },
    "ZCloudsec": {
        "detected": false,
        "result": "clean site"
    },
    "K7AntiVirus": {
        "detected": false,
        "result": "clean site"
    },
    "Quttera": {
        "detected": false,
        "result": "clean site"
    },
    "AegisLab WebGuard": {
```

```
                "detected": false,
                "result": "clean site"
        },
        "MalwareDomainList": {
                "detected": false,
                "result": "clean site",
                "detail":
"http://www.malwaredomainlist.com/mdl.php?search=www.cnet.com"
        },
        "ZeusTracker": {
                "detected": false,
                "result": "clean site",
                "detail": "https://zeustracker.abuse.ch/monitor.php?host=www.cnet.com"
        },
        "zvelo": {
                "detected": false,
                "result": "clean site"
        },
        "Google Safebrowsing": {
                "detected": false,
                "result": "clean site"
        },
        "Kaspersky": {
                "detected": false,
                "result": "clean site"
        },
        "BitDefender": {
                "detected": false,
                "result": "clean site"
        },
        "Opera": {
                "detected": false,
                "result": "clean site"
        },
        "ADMINUSLabs": {
                "detected": false,
                "result": "clean site"
        },
        "C-SIRT": {
                "detected": false,
                "result": "clean site"
        },
        "CyberCrime": {
                "detected": false,
		"result": "clean site"
	},
	"Websense ThreatSeeker": {
		"detected": false,
		"result": "clean site"
	},
	"VX Vault": {
		"detected": false,
		"result": "clean site"
	},
	"Webutation": {
		"detected": false,
		"result": "clean site"
	},
	"Trustwave": {
		"detected": false,
		"result": "unrated site"
	},
	"Web Security Guard": {
		"detected": false,
		"result": "clean site"
	},
	"Dr_Web": {
		"detected": false,
		"result": "clean site"
	},
	"G-Data": {
		"detected": false,
		"result": "clean site"
	},
	"Malwarebytes hpHosts": {
		"detected": false,
		"result": "clean site"
	},
	"Wepawet": {
		"detected": false,
		"result": "clean site"
	},
	"AlienVault": {
		"detected": false,
		"result": "clean site"
	},
	"Emsisoft": {
		"detected": false,
        "result": "clean site"
    },
    "Malc0de Database": {
        "detected": false,
        "result": "clean site",
        "detail": "http://malc0de.com/database/index.php?search=www.cnet.com"
    },
    "SpyEyeTracker": {
        "detected": false,
        "result": "clean site",
        "detail":
"https://spyeyetracker.abuse.ch/monitor.php?host=www.cnet.com"
    },
    "Phishtank": {
        "detected": false,
        "result": "clean site"
    },
    "Malwared": {
        "detected": false,
        "result": "clean site"
    },
    "Avira": {
        "detected": false,
        "result": "clean site"
    },
    "StopBadware": {
        "detected": false,
        "result": "unrated site"
    },
    "Antiy-AVL": {
        "detected": false,
        "result": "clean site"
    },
    "FraudSense": {
        "detected": false,
        "result": "clean site"
    },
    "malwares_com URL checker": {
        "detected": false,
        "result": "clean site"
    },
    "Comodo Site Inspector": {
        "detected": false,
        "result": "clean site"
```

```
},
"Malekal": {
        "detected": false,
        "result": "clean site"
},
"ESET": {
        "detected": false,
        "result": "clean site"
},
"Sophos": {
        "detected": false,
        "result": "unrated site"
},
"Yandex Safebrowsing": {
        "detected": false,
        "result": "clean site",
        "detail": "http://yandex.com/infected?l10n=en&url=http://www.cnet.com/"
},
"SecureBrain": {
        "detected": false,
        "result": "clean site"
},
"Malware Domain Blocklist": {
        "detected": false,
        "result": "clean site"
},
"Netcraft": {
        "detected": false,
        "result": "unrated site"
},
"PalevoTracker": {
        "detected": false,
        "result": "clean site"
},
"CRDF": {
        "detected": false,
        "result": "clean site"
},
"ThreatHive": {
        "detected": false,
        "result": "clean site"
},
"ParetoLogic": {
        "detected": false,
		"result": "clean site"
	},
	"Rising": {
		"detected": false,
		"result": "clean site"
	},
	"URLQuery": {
		"detected": false,
		"result": "unrated site"
	},
	"Sucuri SiteCheck": {
		"detected": false,
		"result": "clean site"
	},
	"Fortinet": {
		"detected": false,
		"result": "unrated site"
	},
	"SCUMWARE_org": {
		"detected": false,
		"result": "clean site"
	},
	"Spam404": {
		"detected": false,
		"result": "clean site"
	}
	}
	},
	"network": {}
```

HTML webpage generated



Category	Started On	Completed On	Duration	Cuckoo Version
URL	2014-07-29 12:31:57	2014-07-29 12:43:47	710 seconds	1.2-dev

Machine	Label	Manager	Started On	Shutdown On
analysis1	Windows	ESX	2014-07-29 12:31:57	2014-07-29 12:43:46

Errors

- **The analysis hit the critical timeout, terminating.**

URL Details

URL	`http://www.cnet.com`
VirusTotal	Permalink VirusTotal Scan Date: 2014-07-29 07:04:45

H. Errors Encountered

Cuckoo Install Errors

Cuckoo Error 1: CuckooCititcalError: unable to ping REsultServer on 192.168.56.1:2804 [error 99] cannot assign requested address.

Fix: ifconfig and found eth0 IP address.

Cuckoo Error 2: CuckooCriticalError:VirtualBox vboxmanage not found at specified path "/usr/bin/vboxmanage/".

Fix: Created a folder named "vmrun" in order to get back the error.

Cuckoo Error 3: CuckooCriticalError: libvirt returned an exception on connection: unsupported configuration: libvirt was built without the esx driver.

Fix:

When installing ESXi onto a machine with a biostar motherboard failed to install by hanging during the initialization of ACPI.

Fix: installed into VMWare Workstation

Virtual Machine Errors:

Ran Cuckoo Sandbox and tested it against the website http://www.cnet.com and once we ran the sandbox we were able to get a clean detection, report and analysis. When we tried to run the test again, we were unable to power on the Windows 7 virtual machine and were receiving an error about lack of space in swap files. We consolidated our snap shots and then we got another error and then we were unable to expand virtual machine disk space due to the fact it was greyed out and un-editable; even with 13GB of extra space

I. System Specifications

Host

- Intel i7 950
- 3.06 Ghz
- 12GB HyperX RAM
- nVidia GeForce 760 FTW

Virtual Machine(Windows)

- Windows 7 64-bit
- Dual-core processor
- 4GB RAM
- 32GB HDD

Virtual Machine(Ubuntu)

- Ubuntu 14.04 64-bit
- Dual-core processor
- 4GB RAM
- 16GB HDD

J. Failures

- Initial install of Cuckoo Box
    - Resolved
- Initial install of Yara onto the standard Cuckoo sandbox layout
- Creating a database of known malware signatures
- Allocating memory between ESXi, Ubuntu vm and Windows vm
    - Resolved
- Killed the test machine
    - Resolved
- Windows vm downgraded to version 8, causing an error reverting to snapshot during Cuckoo testing

K. Successes

- Installed Cuckoo sandbox and successfully configured it
- Ran a test of www.cnet.com, www.espn.com
- examined malware contained in the

L. Future Work

Add configuration to pull from pool of existing virtual machines to replace the infected machine under investigation. In case of the analysis has to run for an extended amount of time the user experience will be minimally disturbed.

Build an onboard repository of known virus hashes and use to speed up the analysis process. By having a repository to look at known cases we will be able to quickly disregard and drop malware that has already been encountered.

Also develop tools to establish a relationship of programs to show the inheritance from older to newer versions of malware analyzed.