UC.yber; Meeting 20

Announcements

- Tomorrow **UCRI** will be hearing out our research ideas
- **IEEE Secure Development Conference** (at MIT) apply by Aug 11th
- **RAPIDS 2** under discussion as State faces funding problems
- Focus on **HS outreach** will as Fall approaches
- What is **SFS**?

If You’re New!

- Join our Slack ucyber.slack.com
- Follow us on Twitter @UCyb3r and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: Content/Events , Finance, and Social Media
- Stay updated through our weekly emails

Last Week

- Had no meeting due to the holiday
- The week before we discussed our NCCDC topics

Malware Sandboxing

What is Cuckoo

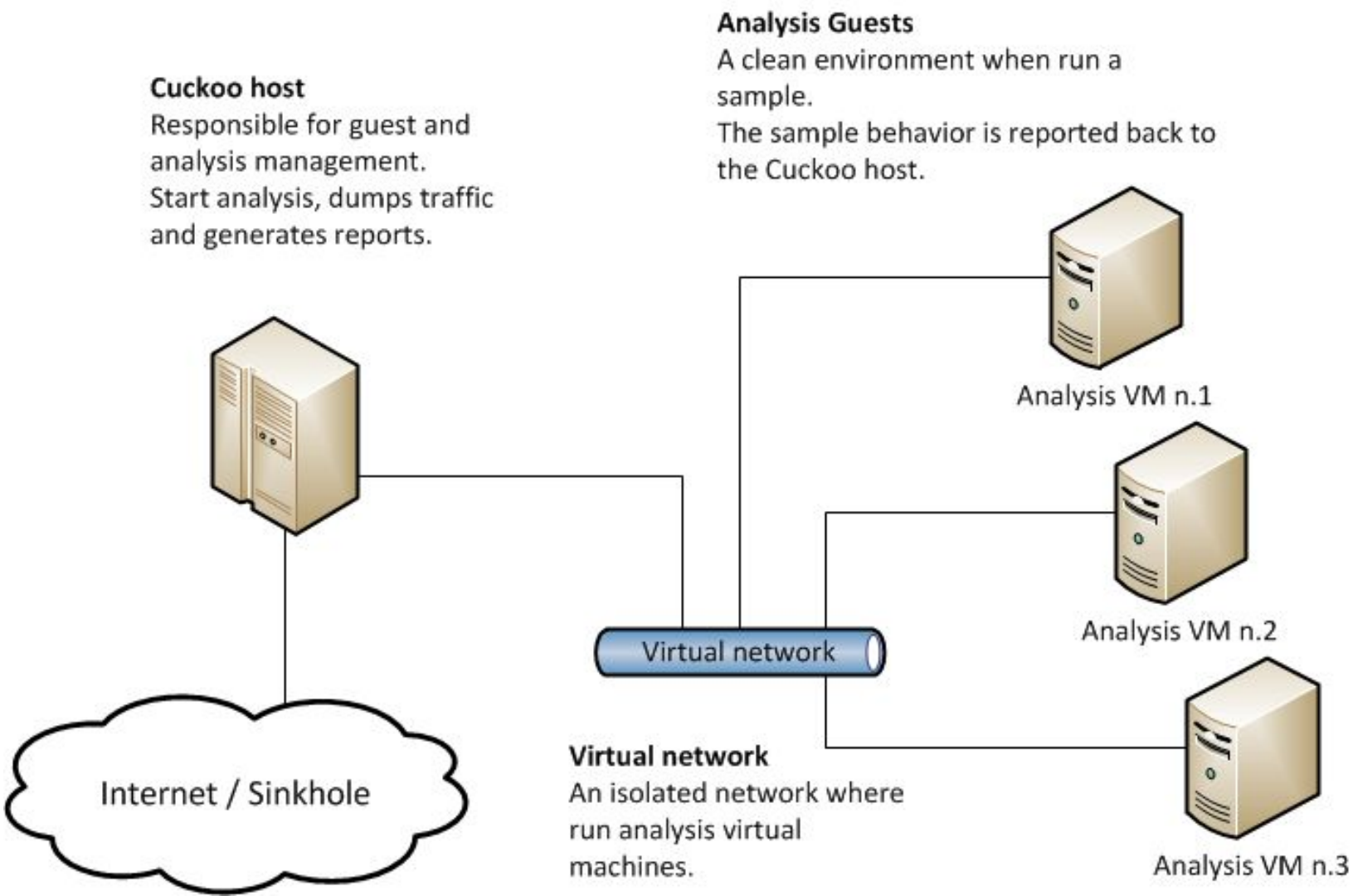
- A **malware analysis** tool
- Sits on top of a VM (like virtualbox)
- Interconnectivity with other malware analysis tools like **Yara**
- Google **Summer of Code** project
- Preferred OS Ubuntu or Debian

What Can Cuckoo Do?

- Traces of **calls performed by all processes** spawned by the malware.
- Files being **created, deleted and downloaded** by the malware during its execution.
- **Memory dumps** of the **malware** processes.
- Network traffic trace in **PCAP** format.
- **Screenshots** taken during the execution of the malware.
- **Full memory dumps** of the machines.

Uses?

- Generic Windows executables
- DLL files
- PDF documents
- Microsoft Office documents
- URLs and HTML files
- PHP scripts
- PHP scripts
- CPL files
- Visual Basic (VB) scripts
- ZIP files
- Java JAR
- Python files
- Almost anything else


Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.
Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.
Analysis VM n.1
Analysis VM n.2
Analysis VM n.3
Virtual network
Internet / Sinkhole
Virtual network
An isolated network where run analysis virtual machines.

Preparing the Host:

- Dual boot latest Linux LTS:
  - https://www.ubuntu.com/download/desktop
    - Download onto hard drive, open and place onto flash drive…..I have one we can pass around if needed
- Load latest Python scripts
  - ```
    sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
    sudo apt-get install python-virtualenv python-setuptools
    sudo apt-get install libjpeg-dev zlib1g-dev swig
    ```
- MongoDB
  - ```
    $ sudo apt-get install mongodb
    ```
- PostgreSQL as database
  - ```
    $ sudo apt-get install postgresql libpq-dev
    ```
    ```

Preparing the Host:

- KVM as machinery module
  - `$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils python-libvirt`
- Cuckoo adopts tcpdump
  - `$ sudo apt-get install tcpdump apparmor-utils`
    `$ sudo aa-disable /usr/sbin/tcpdump`
- For Linux platforms with AppArmor disabled (e.g., Debian) the following command will suffice to install tcpdump:
  - `$ sudo apt-get install tcpdump`
- Tcpdump requires root privileges, but since you don't want Cuckoo to run as root you'll have to set specific Linux capabilities to the binary:
  - `$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump`
- You can verify the results of the last command with:
  - `$ getcap /usr/sbin/tcpdump`
    `**/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip`

Preparing the Host:

- setcap
  - sudo apt-get install libcap2-bin
- **Installing M2Crypto**
  - sudo apt-get install swig

All Done with that!

Installing Cuckoo

- Create a new user:
  - sudo adduser cuckoo
- make sure the new user belongs to the “libvirtd” group (or the group your Linux distribution uses to run libvirt):
  - sudo usermod -a -G libvirtd cuckoo

Installing Cuckoo

- Download it:
  - sudo pip install -U pip setuptools
  - sudo pip install -U cuckoo
  - virtualenv venv
  - venv/bin/activate
  - pip install -U pip setuptools
  - pip install -U cuckoo