Virtualisation for analyze Forensic

Hadrien Hachez, 15306

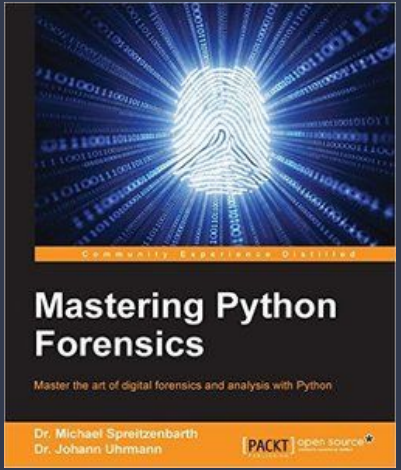

Community Experience Distilled
Mastering Python Forensics
Master the art of digital forensics and analysis with Python
Dr. Michael Spreitzenbarth
Dr. Johann Uhrmann
PACKT open source

Table of Content

- Concepts :
  - forensic analysis
  - virtualization
  - virtualization forensic
- dangers of virtualization
- virtualization as a source of evidence

Concepts

Forensic analysis

“Forensic analysis, in the field of cyber security, consists in carrying out an analysis of the information system after a computer attack.”

3 steps :

1. collect information
2. analyze
3. report

not really something new…

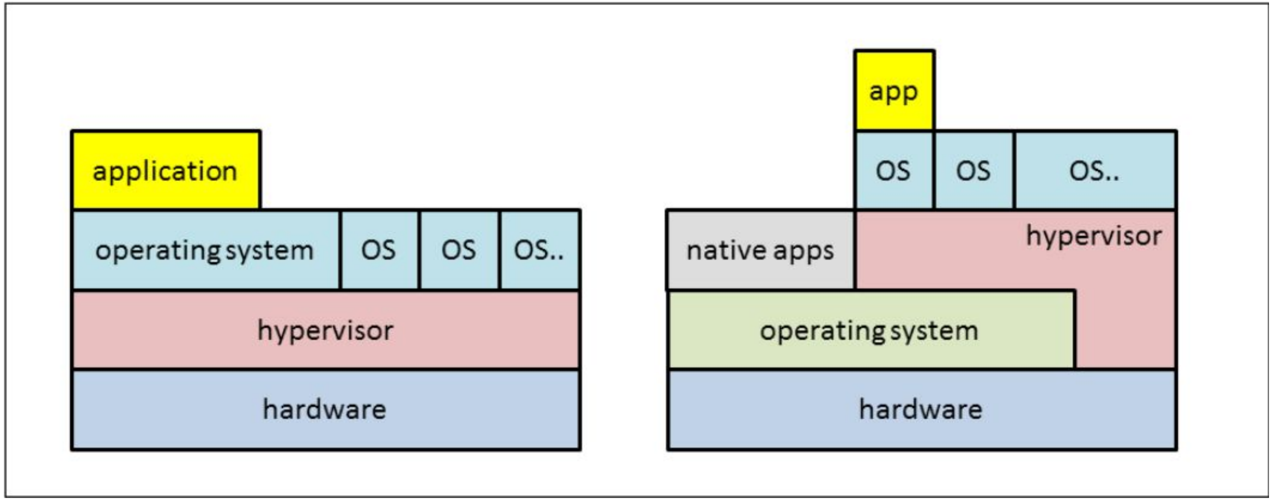
Virtualization

“In computing, **virtualization** refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. “ *Wikipedia*

5 actors :

1. Human
2. Guest system
3. Host system
4. Hypervisor
5. Hardware

Virtualization



bare-metal hypervisor (T1) :
VMware ESXi, Microsoft Hyper-V

desktop virtualization (T2)
Oracle virtual Box, VMware Workstation

Virtualization forensic

Virtualization environments can create snapshots (contains a frozen-in-time state of the system)

Those snapshots can be utilized as a source of forensic data.

Dangers of virtualization

Attacks

ROGUE MACHINE

If an attacker can get access to the hypervisor, he may just create new virtual resources (bridgehead, memory thief). Widespread virtualization environment offers APIs and language bindings to enumerate the virtual machines and other virtual resources of the environment.

CLONING SYSTEM

Traces of abuse of this API**.** Acts like cloning systems generates log files. The log files are saved as compressed archives. We can so easily know past logs and detect anomalies.

Attacks - misuse of virtual resources

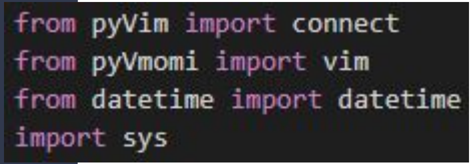
DETECTING ROGUE NETWORK
Due to malicious access to Network virtualization (DCaaS) or human error, resources are available on internet bypassing the firewalls, and allowing access malicious services.

DIRECT HARDWARE ACCESS
Even if direct access to the hypervisor hardware breaks one fundamental principle of virtualization, it happens and a virtual machine can manipulate the virtualization environment.

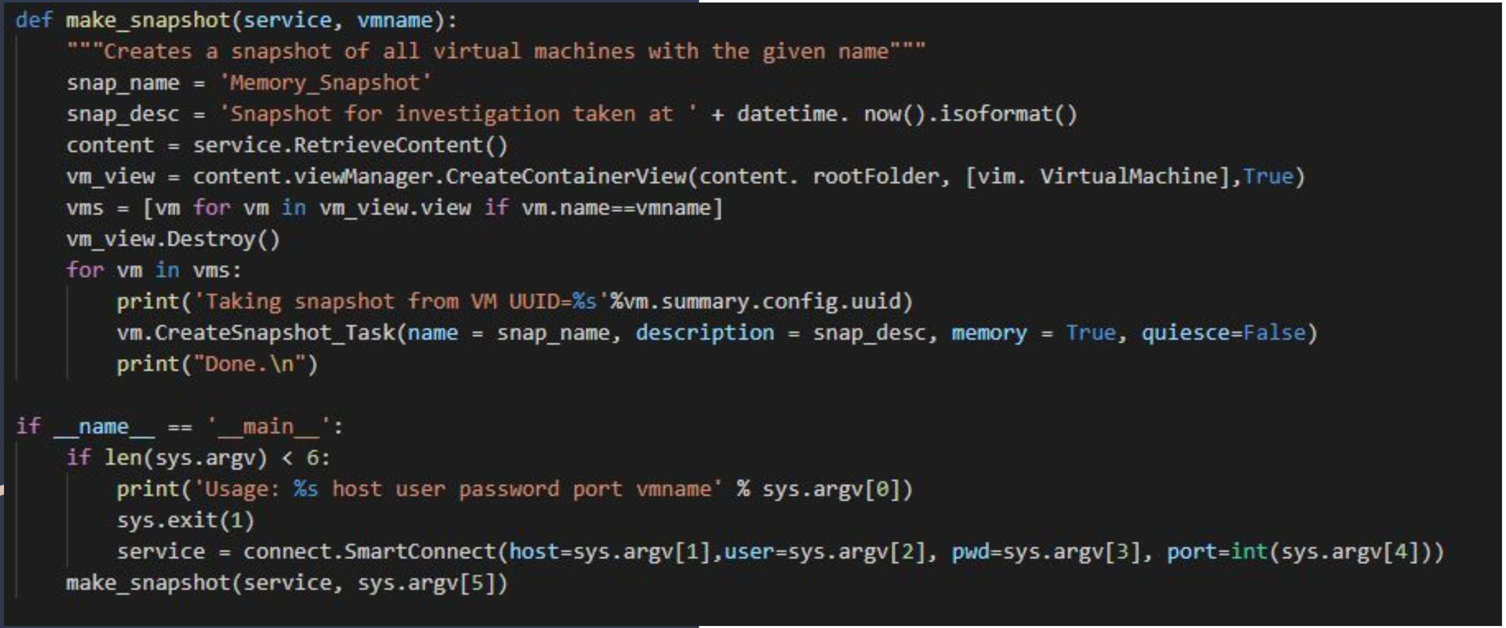
Virtualization as a source of evidence

Virtualization = Source of evidence

CREATING FORENSIC COPIES OF RAM CONTENT



```python
from pyVim import connect
from pyVmomi import vim
from datetime import datetime
import sys
```



```python
def make_snapshot(service, vmname):
    """Creates a snapshot of all virtual machines with the given name"""
    snap_name = 'Memory_Snapshot'
    snap_desc = 'Snapshot for investigation taken at ' + datetime. now().isoformat()
    content = service.RetrieveContent()
    vm_view = content.viewManager.CreateContainerView(content. rootFolder, [vim. VirtualMachine],True)
    vms = [vm for vm in vm_view.view if vm.name==vmname]
    vm_view.Destroy()
    for vm in vms:
        print('Taking snapshot from VM UUID=%s'%vm.summary.config.uuid)
        vm.CreateSnapshot_Task(name = snap_name, description = snap_desc, memory = True, quiesce=False)
        print("Done.\n")

if __name__ == '__main__':
    if len(sys.argv) < 6:
        print('Usage: %s host user password port vmname' % sys.argv[0])
        sys.exit(1)
        service = connect.SmartConnect(host=sys.argv[1],user=sys.argv[2], pwd=sys.argv[3], port=int(sys.argv[4]))
    make_snapshot(service, sys.argv[5])
```

Virtualization = Source of evidence

USING SNAPSHOTS AS DISK IMAGES

creating a forensic disk image usually incorporates taking the system offline

creation of a snapshot of a virtual machine results in basically no downtime

For the forensic analysis, the captured disk images can be connected to a virtual forensic workstation. There, these images can be treated like any other physical hard drive.

The original copies must remain intact in order to provide forensic soundness.

Virtualization = Source of evidence

CAPTURING NETWORK TRAFFIC

The virtualization environment represents virtual machines and Network Interfaces Card (NIC) **AND** the virtual network devices that are needed to interconnect these systems.

For the standard virtual switch : 3 steps

- Create a new port group on this switch to monitor.
- Modify the Security settings of this port group and change the Promiscuous mode to Accept
- Configure the network card of the virtual capture system to the new port group.

Conclusion

Conclusion

What we learned :

- How virtualization changes the landscape not just for IT operations, but also for the attacker and forensic specialist.
- Systems can be created, reshaped, and copied for good and bad reasons.
- How virtualization can be beneficial in getting untampered RAM dumps from the systems that should be analyzed.

Sources

- https://en.wikipedia.org/wiki/Virtualization
- https://www.ossir.org/jssi/jssi2009/3A.pdf
- https://www.hackersrepublic.org/forensic/introduction
- https://latesttrickes.com/wp-content/uploads/2017/12/Mastering-Python-Forensics.pdf
-