CySER Workshop
May 21, 2024

Dr. Clemente Izurieta
Professor of Computer Science
Montana State University

Topic: Digital Forensics

Software:
If you would like to experiment with memory forensics tools, you will need to install Volatility2 and Volatility3 in your laptop. These tools run on a standard Linux OS.

The following instructions are specific to Ubuntu 20.04 (it supports python2 and python3. Note that Ubuntu 24.04 does not support python2), but you can install these tools on your preferred version of a Linux OS.

1. Install your preferred virtualization software on your Laptop and create a Linux VM. (Virtual Box, VMWare Fusion, etc.).

Volatility2

1. Update packages
    a. sudo apt-get update
    b. sudo apt-get upgrade

2. Install Python build tools
    a. sudo apt-get install python-dev
    b. sudo apt-get install python3-dev

3. Install pip for Python 2
    a. curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
    b. sudo python2 get-pip.py
    c. sudo python2 -m pip install -U setuptools wheel

4. Use Python 2 pip to install dependencies
    a. python2 -m pip install -U distorm3 yara pycrypto pillow openpyxl ujson pytz ipython capstone
    b. sudo python2 -m pip install yara

    c. sudo ln -s /usr/local/lib/python2.7/dist-packages/usr/lib/libyara.so /usr/lib/libyara.so

5. Download Volatility2
    a. git clone https://github.com/volatilityfoundation/volatility.git
    b. cd volatility
    c. python2 setup.py build
    d. sudo python2 setup.py build install

6. Validate to make sure you do not have any errors
    a. python2 ./vol.py --info

Volatility3

1. Install dependencies
    a. sudo apt install -y python3 python3-dev libpython3-dev python3-pip python3-setuptools python3-wheel
    b. python3 -m pip install -U distorm3 yara pycrypto pillow openpyxl ujson pytz ipython capstone

2. Download Volatility3
    a. git clone https://github.com/volatilityfoundation/volatility3.git

3. Build and install Volatility3
    a. cd volatility3
    b. python3 setup.py build
    c. sudo python3 setup.py install

4. Validate to make sure you do not have any errors
    a. python3 ./vol.py -h

Memory dumps

We will work with prior captures of memory dumps. The memory dump is the target of the investigation, and I provide them here for this exercise.

Labs are hosted at: https://tinyurl.com/msumfl23
Zip password is: “infected”