Swiss Cyber Forum Kali VM

A Kali VM for Swiss Cyber Forum students

Requirements

- Python 3.x
- Snort 2.x
- SQLite
- sslyze
- Timesketch
- Volatility
- Wireshark
- *Office
- Docker with ELK

Notes

1. Keymap is in **us international**
2. ❗ **not for use in production** ❗
3. sudo without password, 99% of the following commands were run in a root user shell → be a (wo)man

Download

- v1.0 (without TimeSketch) : https://drive.switch.ch/index.php/s/34ZXW2k04NC1qGB - 10.8GB 😳

TO DO FIRST

Things to do to make this VM work on our environment:

1. Download and import into VirtualBox (I didn't test in on VMWare's hypervisors' family, but it should work)
2. Verify or change settings (copy/paste, numbers of CPUs/RAM, Network interfaces - I prefer to bridge them but NAT is OK too, ...) by clicking on the settings buttons
3. snapshot, so the next modifications can be reversed to this state.
4. resize display once logged in (see underneath login/pass) type “display” in the “start menu”, a “Display” application will help you resize the screen to your need

5. Add what you miss (bookmarks/docs/scripts/software/...)

Install

Here's how I installed the VM
From Kali linux Website
https://cdimage.kali.org/kali-2021.2/kali-linux-2021.2-installer-amd64.iso
Standard Install (+ large software selection) on VirtualBox (6.1) with:

- 4096MB RAM
- 50GB Disk (dynamically allocated) - Thank you Docker crap
- 2 Processors
- 1 NIC (Intel Pro/1000)
- Audio
- No floppy 🤣

All in one partition (/ and /home)
One user:

login: scf / pass: scf

User is member of sudoers without password:

```
visudo
```

```
%sudo   ALL=(ALL:ALL) NOPASSWD:ALL
```

Additional tools

Python, SQLite, sslyze, wireshark are already installed

Basic

```
sudo su
apt update && apt upgrade
apt install htop ccze snort -y
```

For snort:
Address range for the local network : ***192.168.0.0/16*** (Default)
To change it:

```
 dpkg-reconfigure snort
```

Volatility

Volatility 2 - Using Pip

Since it's no longer available directly in the repositories... Let's install Volatility2 & 3 alongside

```
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
python2 get-pip.py
apt install python3-pip
apt install pcregrep libpcre++-dev python-dev -y
pip2 install --upgrade setuptools
pip2 install pycrypto
pip2 install distorm3
```

Volatility 2 &3 from github

```
cd
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
python2 get-pip.py
apt install python3-pip pcregrep libpcre++-dev python-dev -y
pip2 install --upgrade setuptools
pip2 install pycrypto
pip2 install distorm3


cd /opt
git clone https://github.com/volatilityfoundation/volatility.git
chmod +x /opt/volatility/vol.py
git clone https://github.com/volatilityfoundation/volatility3.git
ln -s /opt/volatility/vol.py /usr/local/bin/volatility
ln -s /opt/volatility3/vol.py /usr/local/bin/volatility3
```

Docker

```
apt -y install curl gnupg2 apt-transport-https software-properties-common
ca-certificates
echo "deb [arch=amd64] https://download.docker.com/linux/debian buster
stable" | sudo tee  /etc/apt/sources.list.d/docker.list
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
cd
apt update
apt install -y docker-ce docker-ce-cli containerd.io
systemctl enable docker --now
usermod -aG docker scf
curl -s https://api.github.com/repos/docker/compose/releases/latest \
  | grep browser_download_url \
```

```
  | grep docker-compose-Linux-x86_64 \
  | cut -d '"' -f 4 \
  | wget -qi -
mv docker-compose-Linux-x86_64 /usr/bin/docker-compose
chmod +x /usr/bin/docker-compose
```

LibreOffice

```
apt install libreoffice
```

TimeSketch

Manual (Doesn't work)

🔧Fix Me!

```
apt update && apt dist-upgrade
apt install -y openjdk-17-jre-headless apt-transport-https
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key
add -
sudo echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" |
sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list
apt update
apt install -y elasticsearch
systemctl daemon-reload
systemctl enable elasticsearch --now
apt install -y postgresql python3-psycopg2 ## already installed
echo "local   all             timesketch                              md5"
>> /etc/postgresql/13/main/pg_hba.conf
systemctl start postgresql
apt install -y python3-pip python-dev libffi-dev ##already installed
pip3 install timesketch
cp /usr/local/share/timesketch/timesketch.conf /etc/
chmod 600 /etc/timesketch.conf
tsctl add_user -u <username> ## error
```

Docker container

```
cd /opt
git clone https://github.com/google/timesketch.git
```

Launch

❗ As normal user (scf) ❗

```
cd /opt/timesketch
cd docker/dev
sudo docker-compose up # 3h
```

Future addition

- iftop
- molock
- cyberchef
- Posters SANS
- ...

References

- https://netsidetech.ca/2021/02/07/how-to-install-volatility-in-kali/
- https://bootstrap.pypa.io/pip/2.7/
- https://volatility3.readthedocs.io/en/latest/
- https://github.com/volatilityfoundation/volatility/wiki/Installation
- https://www.kali.org/docs/containers/installing-docker-on-kali/
- https://computingforgeeks.com/install-docker-and-docker-compose-on-kali-linux/
- https://cybertheta.blogspot.com/2017/08/how-to-install-libreoffice-in-kali-linux.html
- https://github.com/google/timesketch/blob/907c5eec69cd49b4335ca663c7bf51508fdc8d70/docs/Installation.md

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/os/kali/scf

Last update: **2021/12/29 21:03**