Introduction

Kali VM for course/exercises
Based on Kali 2022.1 &.2 .3

Notes

1. Default Keymap is in **English us** use the menu and type keyboard to change in a GUI
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 ! run as root

VM

From: Kali VMs Images
Docs: Virtualbox Doc
Unzip the file downloaded then import the .vbox file, using “Add” in Virtualbox.

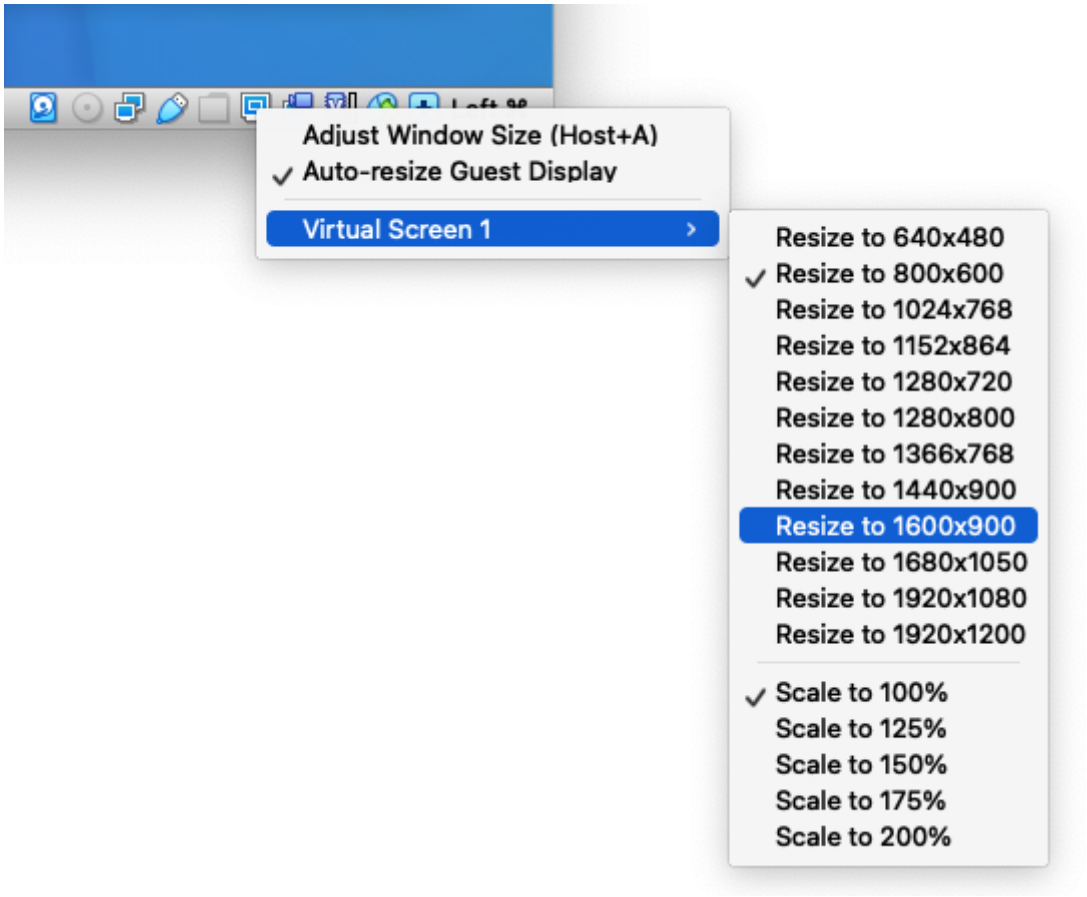
TO DO FIRST

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

1. Download and import into VirtualBox (I didn't test it in on VMWare's hypervisors' family, but it should work, same for UTM/KVM/Proxmox)
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 the original 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 - also check underneath on Display size to make it correct
5. Add what you miss (bookmarks/docs/scripts/software/…)

Display size

using Display in Settings and set it up doesn't work as Virtualbox tries to resize it (for your security …). You need to set it up by hand:



Lock screen

Menu > Settings > Power Manager then in the Tab “Security”:

- Automatically lock the session: Never
- Uncheck “Lock screen when system is going to sleep”

Missing packages

```
sudo su
```

Then as root

```
apt update && apt install -y htop ccze dfc iftop libreoffice libreoffice-l10n-de libreoffice-l10n-fr clipit zaproxy
```

Autologin

Here for the **kali** user, replace by yours if you made another

```
 vi /etc/lightdm/lightdm.conf
```

```
[Seat:*]
```

```
autologin-user=kali
autologin-user-timeout=0
```

New user (OPTIONAL)

```
 useradd -m warnaud
usermod -aG
ad,dialout,cdrom,floppy,sudo,audio,dip,video,plugdev,netdev,wireshark,blueto
oth,kali-trusted,scanner,vboxsf,kaboxer warnaud
chsh -s /usr/bin/zsh warnaud
passwd warnaud
```

Log-out and log in to update all **ENV** variables ($SHELL etc ...)

SUDO

The group **kali-trusted** can launch sudo commands without password

```
 usermod -aG kali-trusted kali
```

Note: replace kali by your user if you prefer to have a dedicated user

Additional packages

Docker

 doesn't work on ARM64 arch  **ONLY for x86_64**

```
apt install -y curl gnupg2 apt-transport-https ca-certificates
echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-
keyring.gpg] https://download.docker.com/linux/debian bullseye stable" |
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor
-o /usr/share/keyrings/docker-archive-keyring.gpg
cd
apt update
apt install -y docker-ce docker-ce-cli containerd.io
systemctl enable docker --now
usermod -aG docker kali
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
```

Python2

```
sudo apt install -y python2 python2.7-dev libpython2-dev
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
sudo python2 get-pip.py
sudo python2 -m pip install -U setuptools wheel
```

Volatility

```
cd /opt
git clone https://github.com/volatilityfoundation/volatility.git
echo "#! /usr/bin/bash
/usr/bin/python2  /opt/volatility/vol.py \$@" > /usr/local/bin/volatility
chmod +x /usr/local/bin/volatility
git clone https://github.com/volatilityfoundation/volatility3.git
ln -s /opt/volatility3/vol.py /usr/local/bin/volatility3

python2 -m pip install -U distorm3 yara pycrypto pillow openpyxl pytz
ipython capstone
python2 -m pip install -U --no-use-pep517 ujson
sudo python2 -m pip install yara
sudo ln -s /usr/local/lib/python2.7/dist-packages/usr/lib/libyara.so
/usr/lib/libyara.so
```

Yara rules

```
mkdir /opt/yara
cd /opt/yara
git clone https://github.com/Yara-Rules/rules.git
```

Volatility-check script

```
cd /opt
git clone https://gitlab.com/arnaud.fortier/volatility-check.git
chmod o+x /opt/volatility-check/volatility-check.sh
ln -s /opt/volatility-check/volatility-check.sh /usr/local/volatility-check
```

Snort

First try

From : Github nullsecurity

```
apt install dh-autoreconf pkg-config cmake
cd /opt
git clone https://github.com/snort3/libdaq.git
cd libdaq
./bootstrap
./configure
make install
ldconfig

cd /opt
git clone https://github.com/snort3/snort3.git
cd snort3
./configure\_cmake.sh --prefix=$HOME/install/snort3 --enable-unit-tests
```

DOESN'T work...

Second try

From: https://upcloud.com/resources/tutorials/installing-snort-on-debian

```
apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev
openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet autoconf
libtool
cd /opt
mkdir snort_src
cd snort_src
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
tar xvzf daq-2.0.7.tar.gz
cd daq-2.0.7
autoreconf -f -i
./configure && make && make install
cd /opt/snort_src
wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
tar xvzf snort-2.9.20.tar.gz
cd snort-2.9.20
./configure --enable-sourcefire CPPFLAGS="-I /usr/include/tirpc" && make &&
make install
ldconfig
groupadd snort
useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
mkdir -p /etc/snort/rules
mkdir -p /var/log/snort
mkdir -p /usr/local/lib/snort_dynamicrules
chmod -R 5775 /etc/snort
chmod -R 5775 /var/log/snort
chmod -R 5775 /usr/local/lib/snort_dynamicrules
chown -R snort:snort /etc/snort
```

```
chown -R snort:snort /var/log/snort
chown -R snort:snort /usr/local/lib/snort_dynamicrules
touch /etc/snort/rules/white_list.rules
touch /etc/snort/rules/black_list.rules
touch /etc/snort/rules/local.rules
cp /opt/snort_src/snort-2.9.20/etc/*.conf* /etc/snort
cp /opt/snort_src/snort-2.9.20/etc/*.map /etc/snort
cd /opt/snort_src
wget https://www.snort.org/rules/community -O ./community.tar.gz
tar xvzf community.tar.gz
cp /opt/snort_src/community-rules/* /etc/snort/rules
sudo sed -i 's/include $RULE_PATH/#include $RULE_PATH/'
/etc/snort/snort.conf
vi /etc/snort/snort.conf
```

DOESN'T WORK EITHER !!!!

Third try

From : https://unix.stackexchange.com/questions/584144/unable-to-locate-package-snort - modified to reflect last Debian 11 version

```
vi /etc/apt/sources.list
```

```
deb http://httpredir.debian.org/debian bullseye main
```

bullseye as kali is now rolling release so put a current version **might → testing** doesn't work ! (as of 20/07/2022)

```
apt update
apt install snort
```

comment the line **deb http://httpredir.debian.org/debian bullseye main**

Configure

```
dpkg-reconfigure snort
```

You can change the default IP range of $HOME_NET (**default is 10.0.2.0/24** aka VirtualBox's VLAN)

Test

```
 vi /etc/snort/rules/local.rules
```

```
alert tcp any any -> any any (msg:"Basic test please comment in
local.rules"; sid:10000001; rev:001;)
```

```
snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf
```

Now launch a web browser or anything that goes on the internet using tcp stack

Update

Uncomment the line in **/etc/apt/sources.list** with debian repos then **apt update && apt upgrade snort**

Brave

```
apt install apt-transport-https curl

sudo curl -fsSLo /usr/share/keyrings/brave-browser-archive-keyring.gpg
https://brave-browser-apt-release.s3.brave.com/brave-browser-archive-
keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/brave-browser-archive-keyring.gpg
arch=amd64] https://brave-browser-apt-release.s3.brave.com/ stable
main"|sudo tee /etc/apt/sources.list.d/brave-browser-release.list

apt update

apt install brave-browser
```

Nala

You can add Nala following the instructions from their Wiki on any Debian/Ubuntu VMs

```
echo "deb https://deb.volian.org/volian/ scar main" | sudo tee
/etc/apt/sources.list.d/volian-archive-scar-unstable.list
wget -qO - https://deb.volian.org/volian/scar.key | sudo tee
/etc/apt/trusted.gpg.d/volian-archive-scar-unstable.gpg > /dev/null
apt update
apt install nala
```

Exam preparation

You can quickly script the files where you'll answer the challenge for the exam:

```
FIRSTNAME="Arnaud"; LASTNAME="Fortier";for challenge in {1..10}; do mkdir -p
~/Desktop/Challenges/${challenge};\
 touch ~/Desktop/Challenges/${challenge}/CSS2024\ $FIRSTNAME\ $LASTNAME\ -\
Challenge${challenge}.docx; done
```

 Change FIRSTNAME/LASTNAME values 

Detailed installation

(if you install from scratch with the ISO - not needed if you already imported the OVA/premade images)

visudo

css user is member of the sudo group

```
sudo visudo
```

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

Virtualbox Additions tools

 not mandatory, only for barebone install, images from Kali have necessary tools already installed Insert the virtual CD  DOESN'T work on Silicon ... (20241028)

```
cd /media/cdrom0
sudo  bash ./VBoxLinuxAdditions.run
sudo usermod -aG vboxsf kali
```

HyperV

Under hyperV you should set this option to get the most of the VM

```
C:\Windows\system32> Set-VM "Kali Linux" -EnhancedSessionTransportType
HVSocket
```

Slow Web browser

if your web browser seems laggy or make your whole VM laggy, just activate the 3D acceleration: **Settings > Display** and check “Enable 3D acceleration”

References

- https://computingforgeeks.com/install-docker-and-docker-compose-on-kali-linux/
- https://seanthegeek.net/1172/how-to-install-volatility-2-and-volatility-3-on-debian-ubuntu-or-kali-linux/
- https://isc.sans.edu/forums/diary/Using+Yara+rules+with+Volatility/22950/
- https://bin3xish477.medium.com/installing-snort-on-kali-linux-9c96f3ab2910