

Kali Linux for CSP/CSS

Kali Linux install for Virtualbox on **Apple Silicon** M1/M2/M3/M4?

For x86_64 → [go here](#)

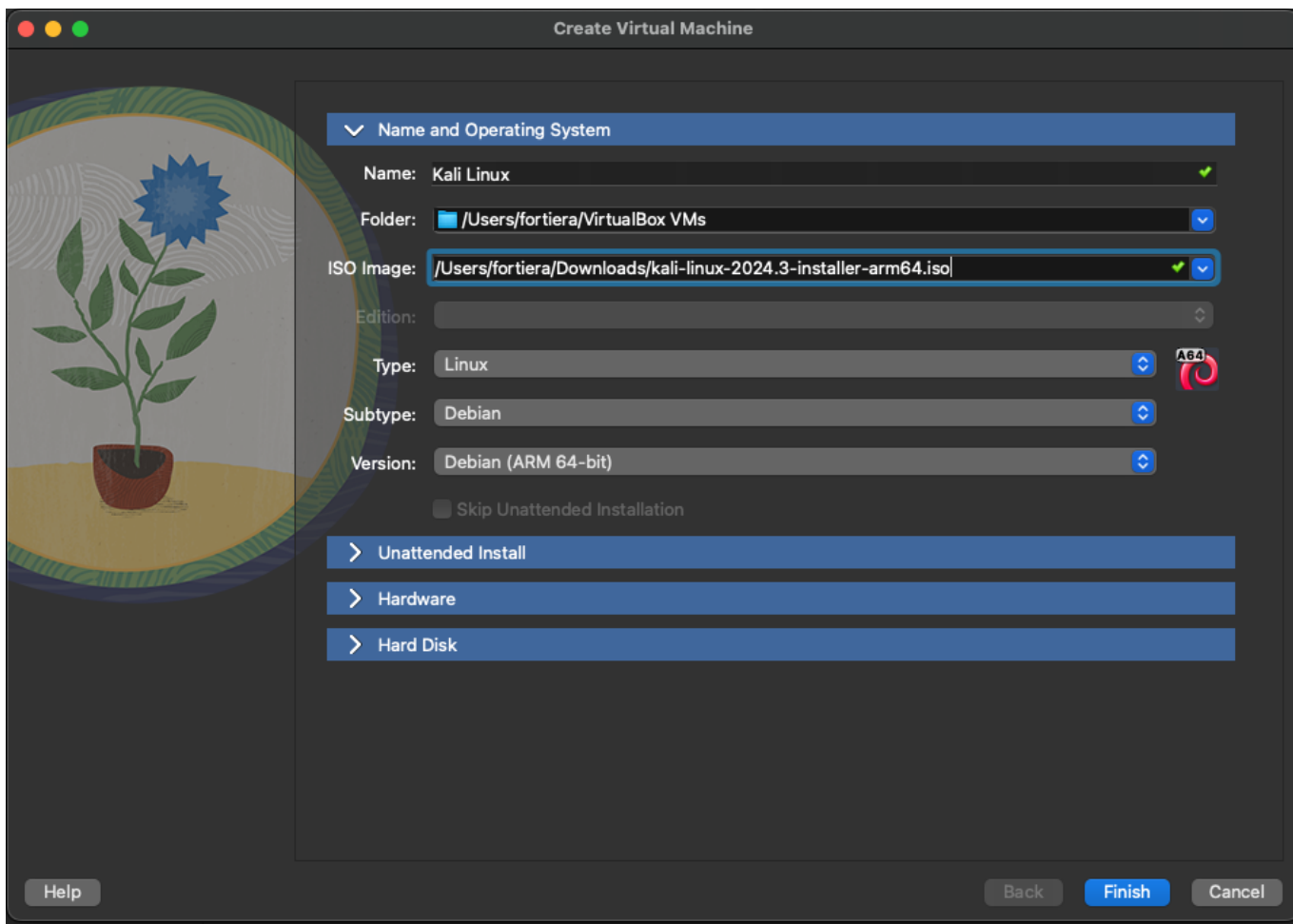


Prerequisite

- Apple Silicon MX CPU
- [Virtualbox Apple Silicon Hosts](#)
- [VirtualBox Extension Pack](#)
- Kali ARM iso install [Apple Silicon \(ARM64\)](#)

Install

Create a VM using the iso as bootable CD



Launch the machine



select language



Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	ཇོངཀལ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

Screenshot

Go Back

Continue

select country



Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

- India
- Ireland
- Israel
- New Zealand
- Nigeria
- Philippines
- Seychelles
- Singapore
- South Africa
- United Kingdom
- United States
- Zambia
- Zimbabwe
- other

Screenshot

Go Back

Continue



Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Select the continent or region to which your location belongs.

Continent or region:

- Africa
- Antarctica
- Asia
- Atlantic Ocean
- Caribbean
- Central America
- Europe**
- Indian Ocean
- North America
- Oceania
- South America

Screenshot

Go Back

Continue



Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.

Country, territory or area:

- Romania
- Russian Federation
- San Marino
- Serbia
- Slovakia
- Slovenia
- Spain
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Ukraine
- United Kingdom
- Åland Islands

Screenshot

Go Back

Continue

locales



Configure locales

There is no locale defined for the combination of language and country you have selected. You can now select your preference from the locales available for the selected language. The locale that will be used is listed in the second column.

Country to base default locale settings on:

Hong Kong	-	en_HK.UTF-8
India	-	en_IN
Ireland	-	en_IE.UTF-8
Israel	-	en_IL
New Zealand	-	en_NZ.UTF-8
Nigeria	-	en_NG
Philippines	-	en_PH.UTF-8
Seychelles	-	en_SC.UTF-8
Singapore	-	en_SG.UTF-8
South Africa	-	en_ZA.UTF-8
United Kingdom	-	en_GB.UTF-8
United States	-	en_US.UTF-8
Zambia	-	en_ZM
Zimbabwe	-	en_ZW.UTF-8

Screenshot Help Go Back **Continue**

Keyboard mapping



Configure the keyboard

Keymap to use:

- American English**
- Albanian**
- Arabic**
- Asturian**
- Bangladesh**
- Belarusian**
- Bengali**
- Belgian**
- Berber (Latin)**
- Bosnian**
- Brazilian**
- British English**
- Bulgarian (BDS layout)**
- Bulgarian (phonetic layout)**
- Burmese**
- Canadian French**
- Georgian Mkhedruli**

Screenshot

Go Back

Continue

or



Configure the keyboard

Keymap to use:

- Portuguese
- Punjabi
- Romanian
- Russian
- Serbian (Cyrillic)
- Sindhi
- Sinhala
- Slovak
- Slovenian
- Spanish
- Swedish
- Swiss French**
- Swiss German
- Tajik
- Tamil
- Telugu
- Thai

Screenshot

Go Back

Continue

machine name



Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot

Go Back

Continue

user (sudoer) + password



Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot

Go Back

Continue



Set up users and passwords

Make sure to select a strong password that cannot be guessed.
Choose a password for the new user:

Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

Show Password in Clear

Screenshot

Go Back

Continue

Partitioning



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk**
- Guided - use entire disk and set up LVM**
- Guided - use entire disk and set up encrypted LVM**
- Manual**

Screenshot

Go Back

Continue



Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI1 (0,0,0) (sda) - 21.5 GB VBOX HARDDISK

Screenshot

Go Back

Continue



Partition disks

Selected for partitioning:

SCSI1 (0,0,0) (sda) - VBOX HARDDISK: 21.5 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)

Separate /home partition

Separate /home, /var, and /tmp partitions

Screenshot

Go Back

Continue



Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Guided partitioning

Configure software RAID

Configure the Logical Volume Manager

Configure encrypted volumes

Configure iSCSI volumes

SCSI1 (0,0,0) (sda) - 21.5 GB VBOX HARDDISK

>		1.0 MB			FREE SPACE	
>	#1	536.9 MB	B	f	ESP	
>	#2	19.9 GB	f	ext4	/	
>	#3	1.0 GB	f	swap	swap	
>		1.0 MB			FREE SPACE	

Undo changes to partitions

Finish partitioning and write changes to disk

Screenshot

Help

Go Back

Continue



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI1 (0,0,0) (sda) as ESP
partition #2 of SCSI1 (0,0,0) (sda) as ext4
partition #3 of SCSI1 (0,0,0) (sda) as swap

Write the changes to disks?

No

Yes

Screenshot

Continue

Default packages



Software selection

At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

Choose software to install:

- Desktop environment [selecting this item has no effect]
- ... Xfce (Kali's default desktop environment)
- ... GNOME
- ... KDE Plasma
- Collection of tools [selecting this item has no effect]
- ... top10 -- the 10 most popular tools
- ... default -- recommended tools (available in the live system)

Screenshot

Continue



Finish the installation

i *Installation complete*
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Please choose <Continue> to reboot.

Screenshot

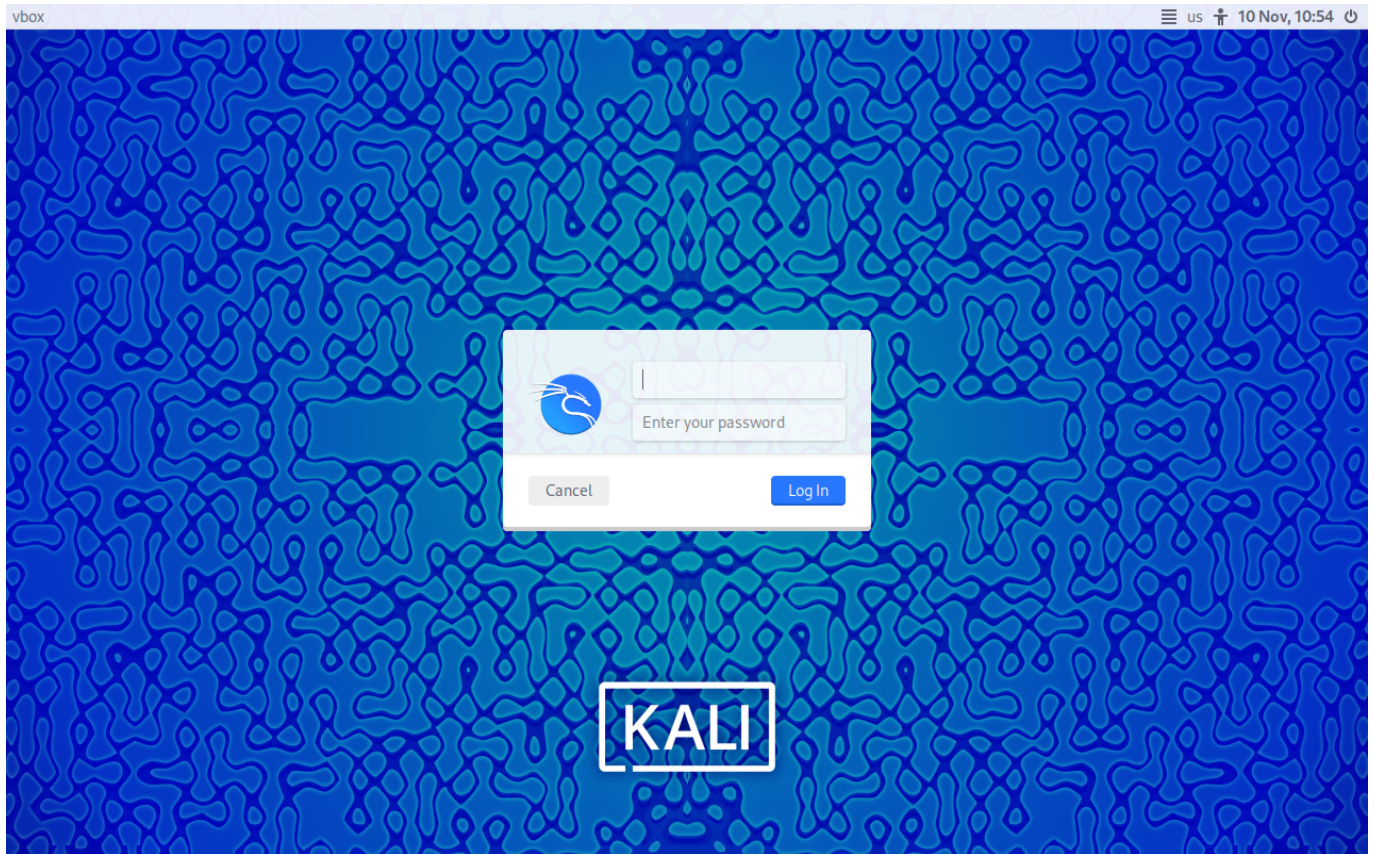
Go Back

Continue

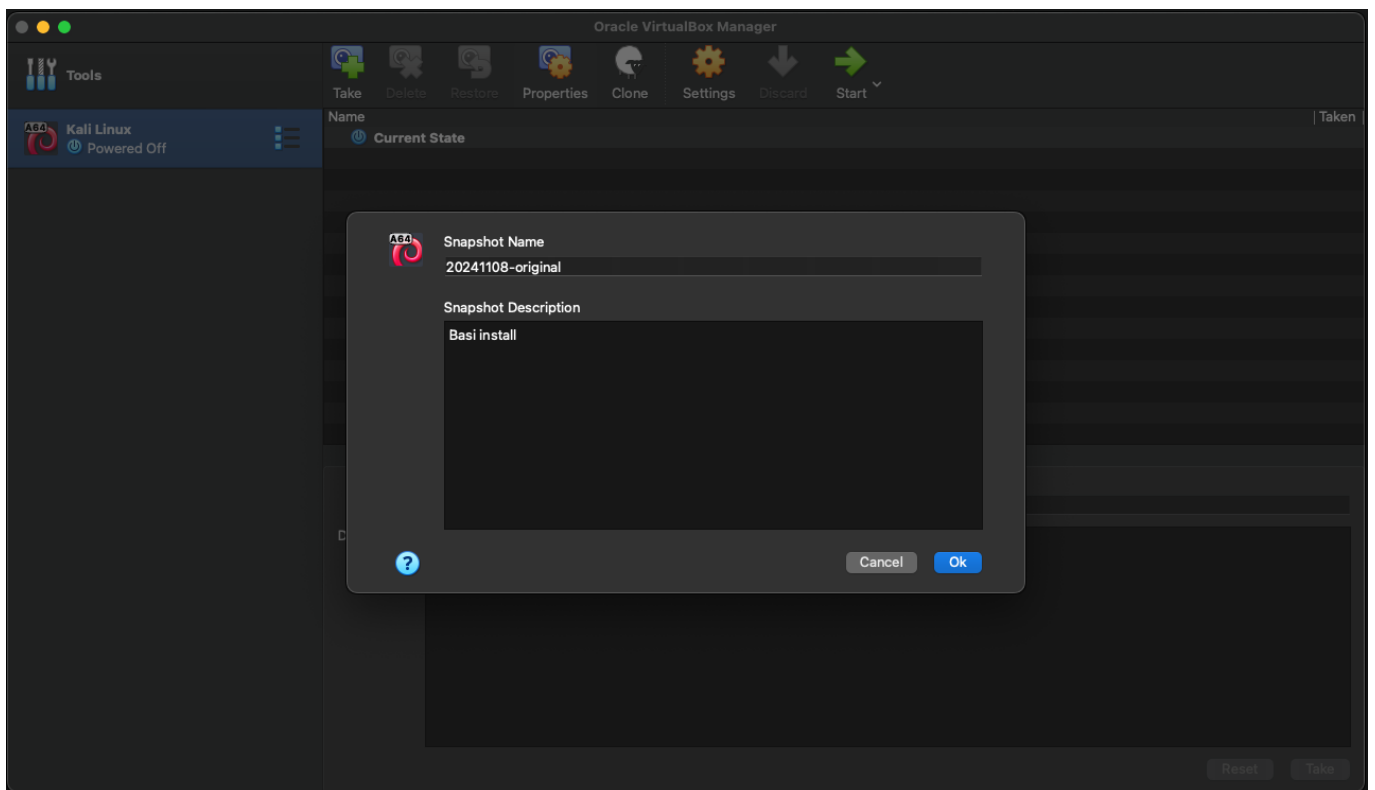
First reboot

check your login/pass then shutdown the VM





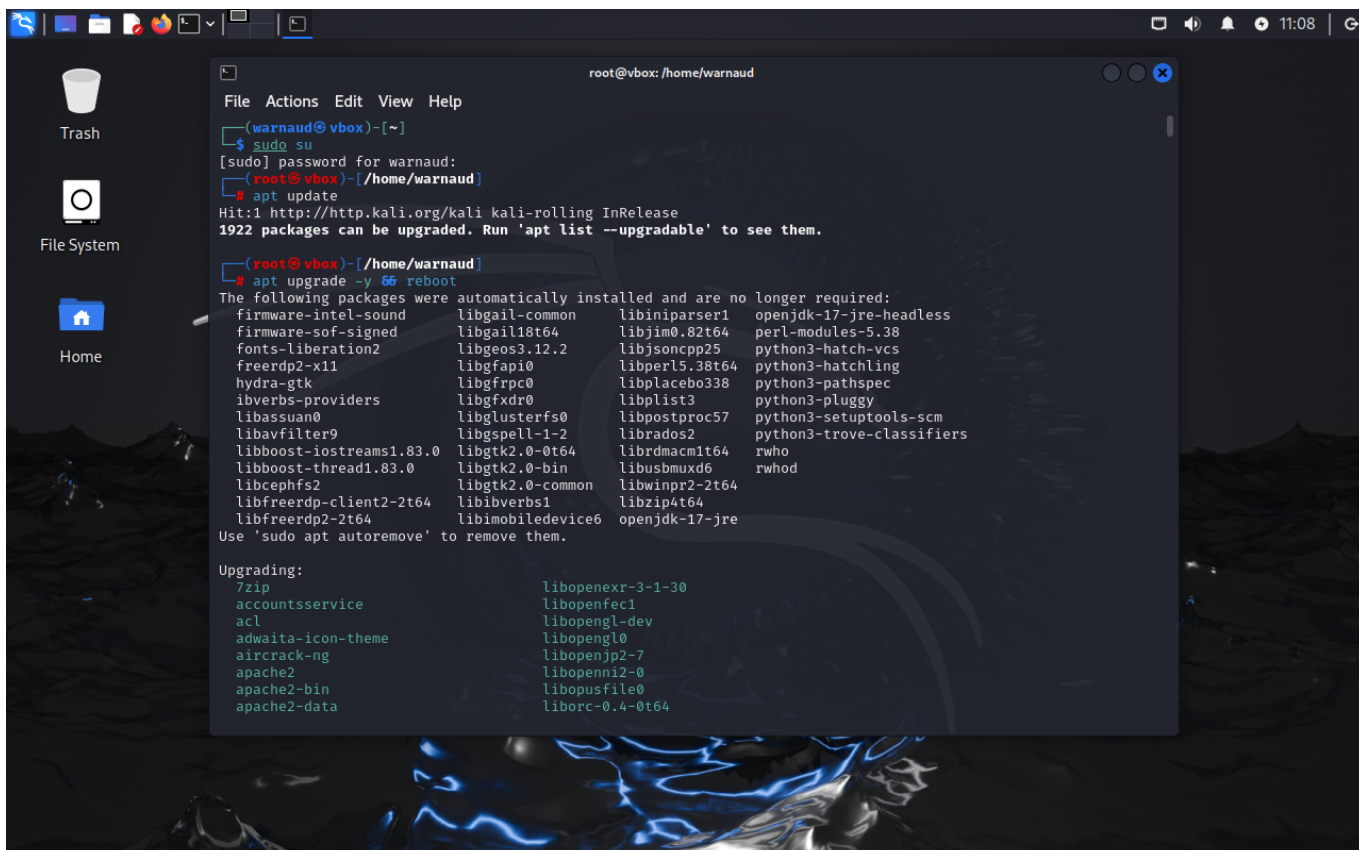
Snapshot



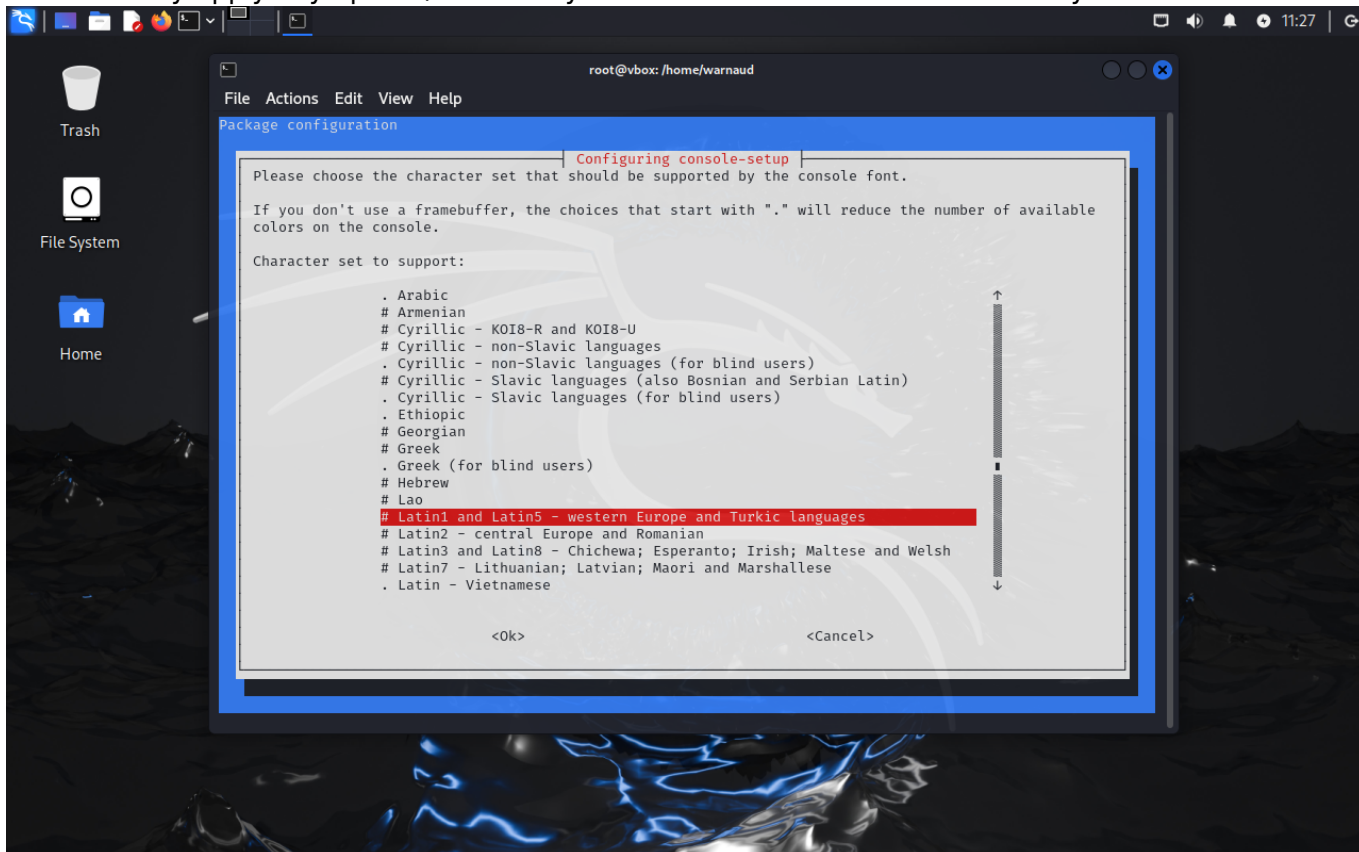
First full upgrade

```
sudo su
```

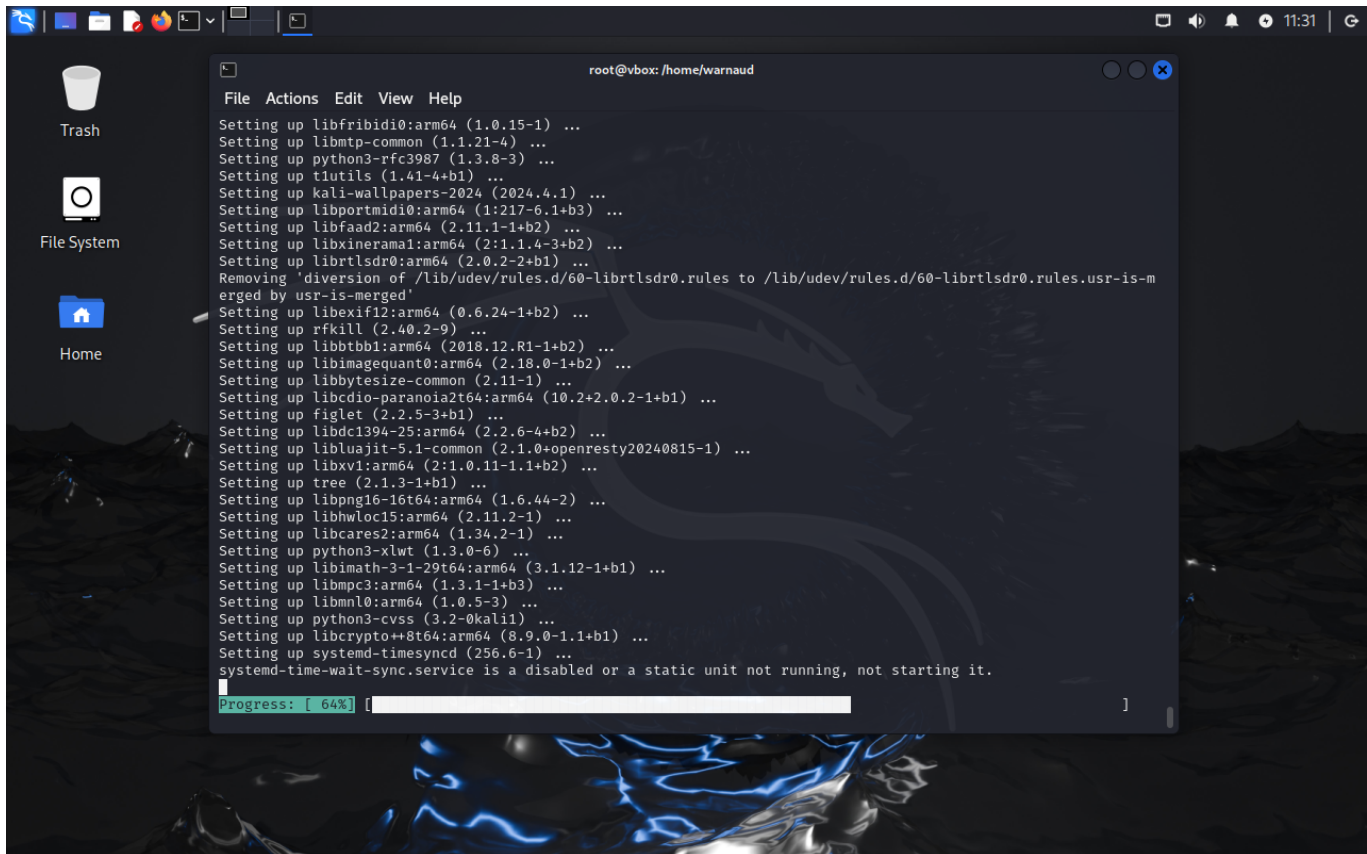
apt update
apt dist-upgrade -y && reboot



we can safely apply any update/restart any services set default values as nobody but us is on this VM



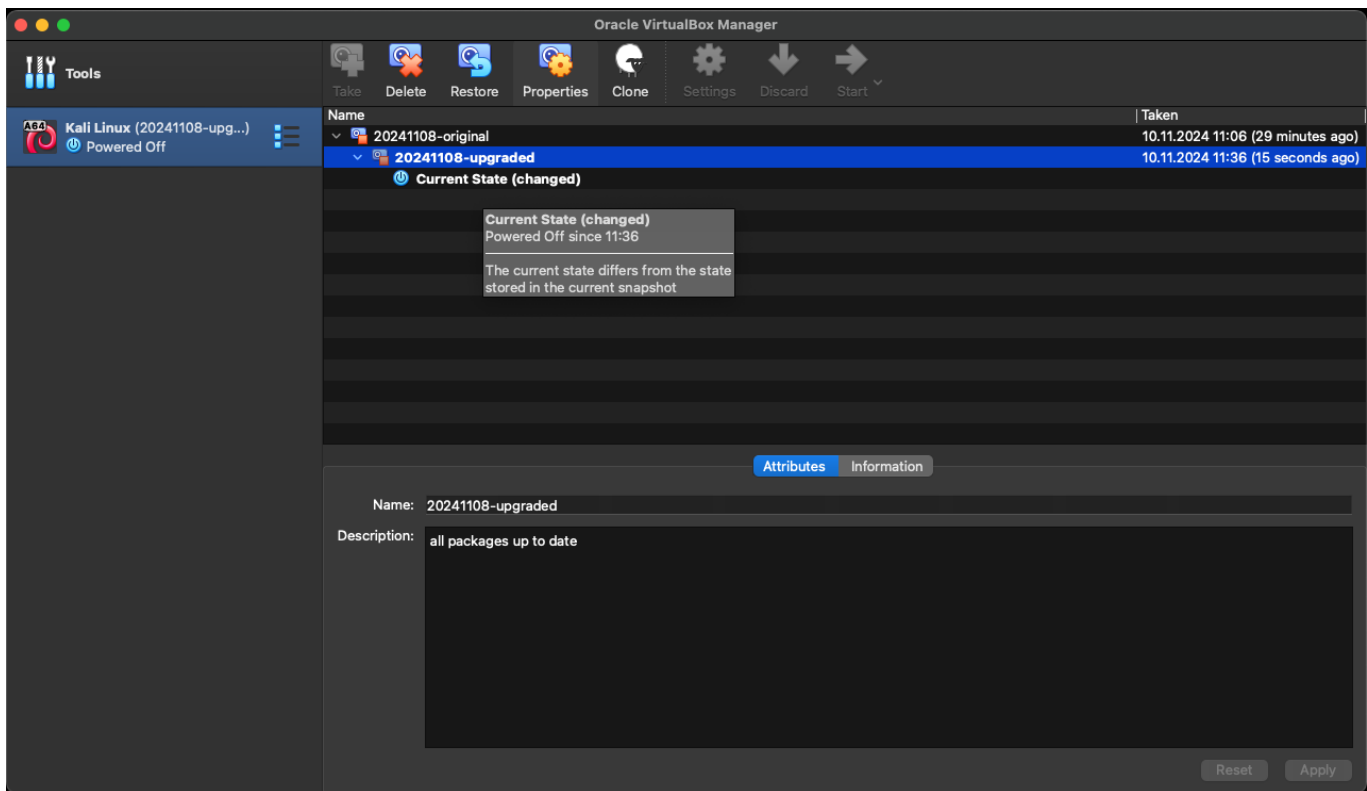
...



Takes a while but should finish then immediately reboot. If it doesn't reboot, note the error and google/Ai for it

snapshot II

shutdown the machine and make a new snapshot

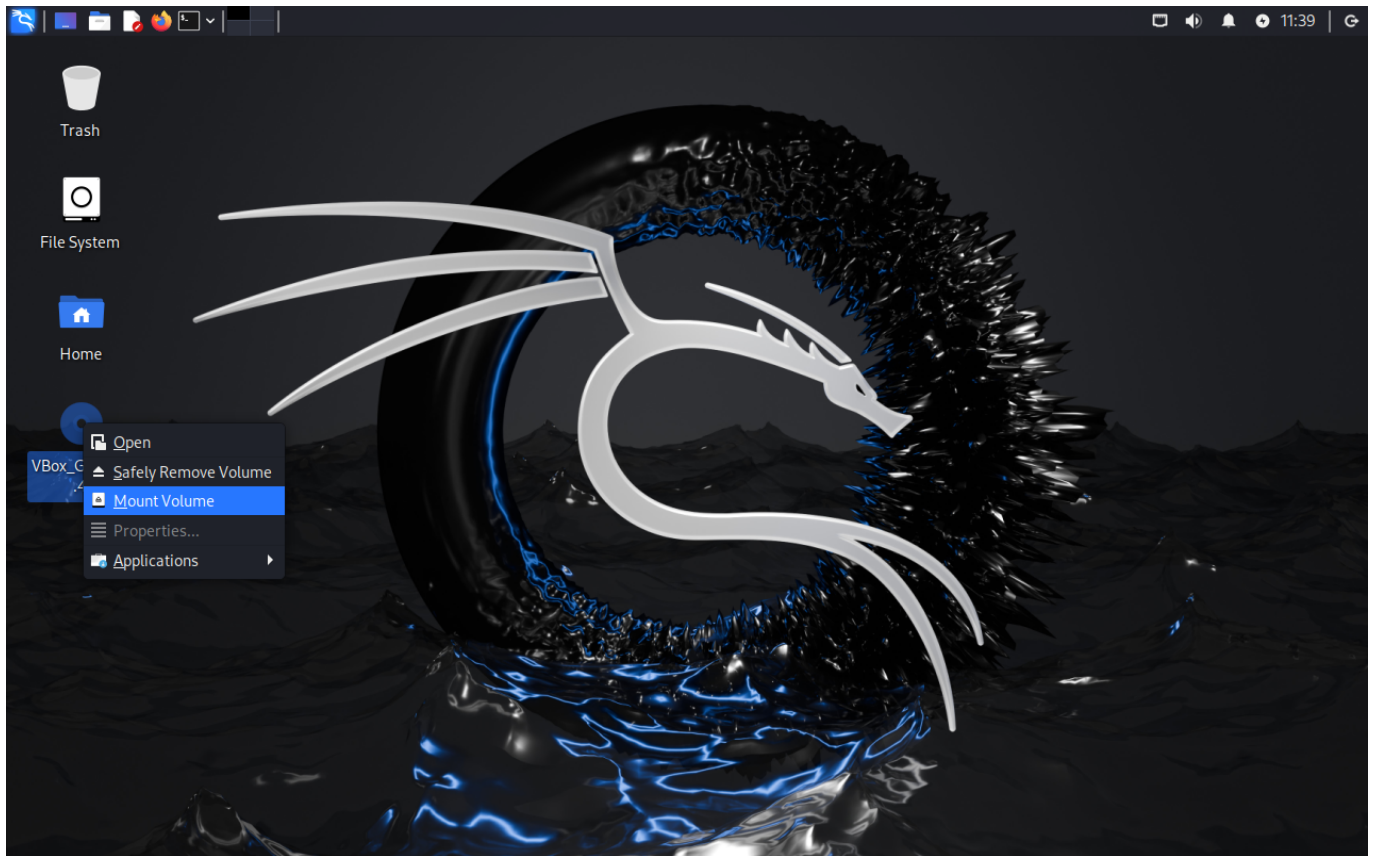


Guest Tools installation

boot the VM, log in your session

click on the menu Devices> Insert Guest Addition CD

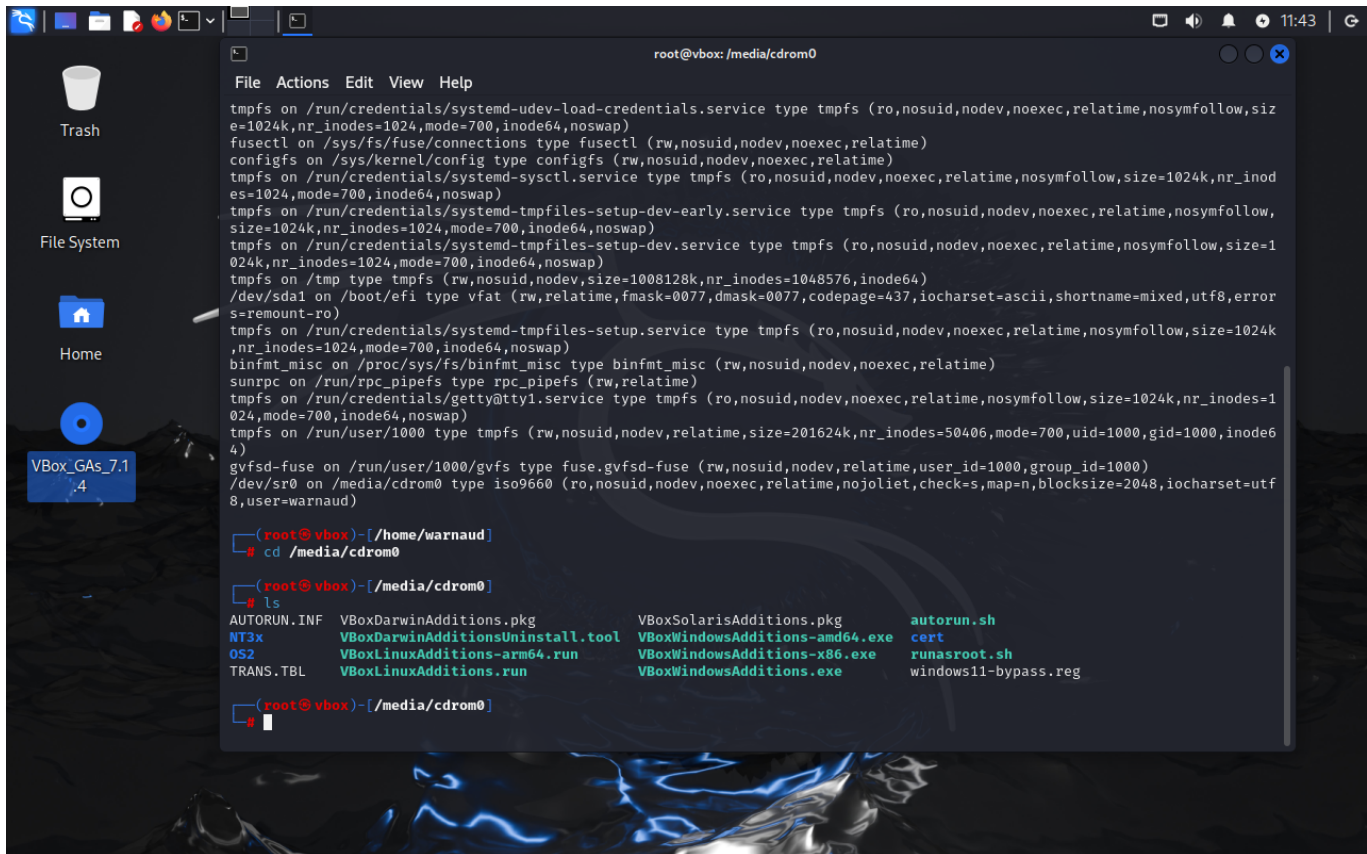
Right-click on the CD on the Desktop and choose "Mount Volume"



Launch a terminal

```
sudo su
```

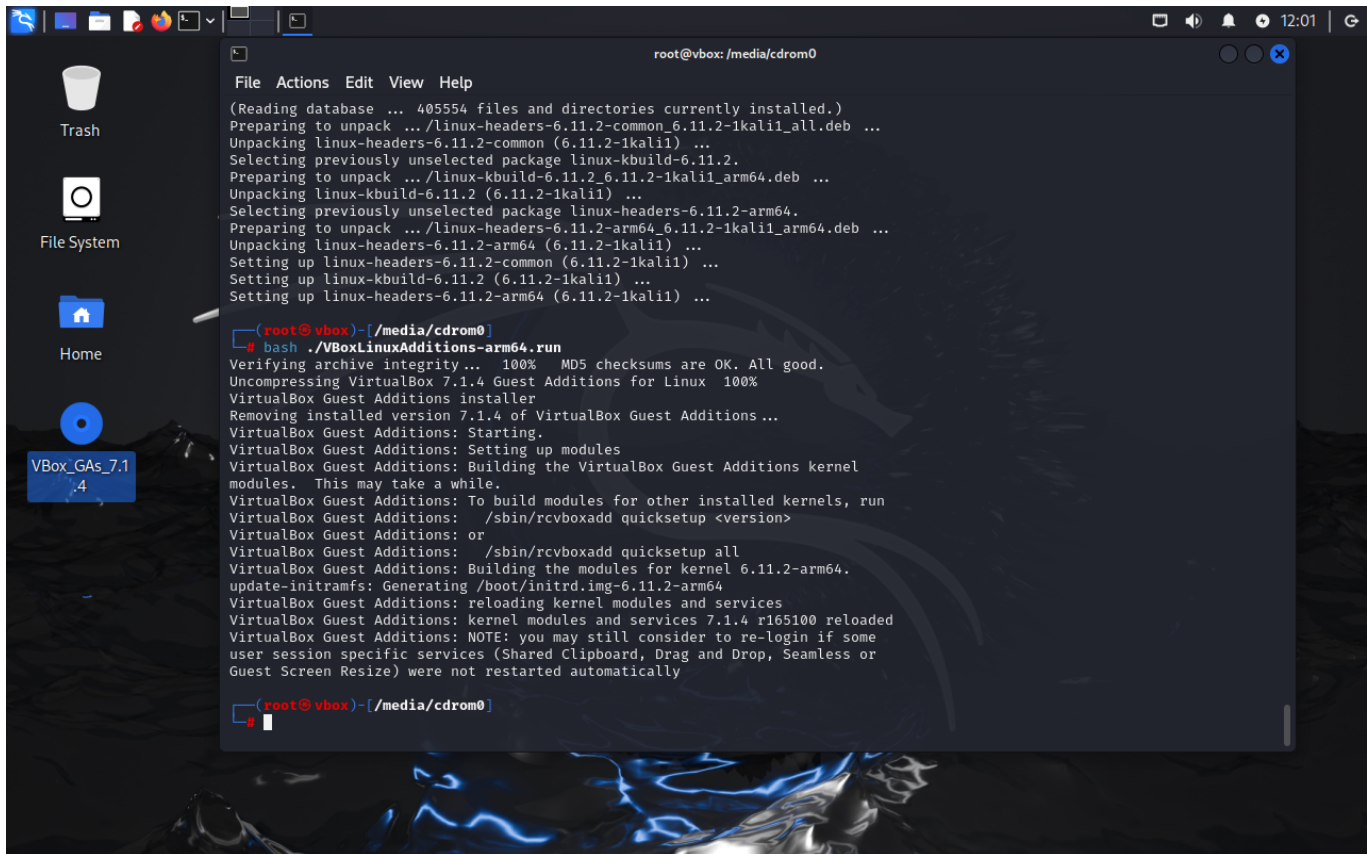
```
cd /media/cdrom0
```



```

apt install -y dkms linux-headers-`uname -r` build-essential
sh ./VBoxLinuxAdditions-arm64.run
usermod -sG vboxsf warnaud
  
```

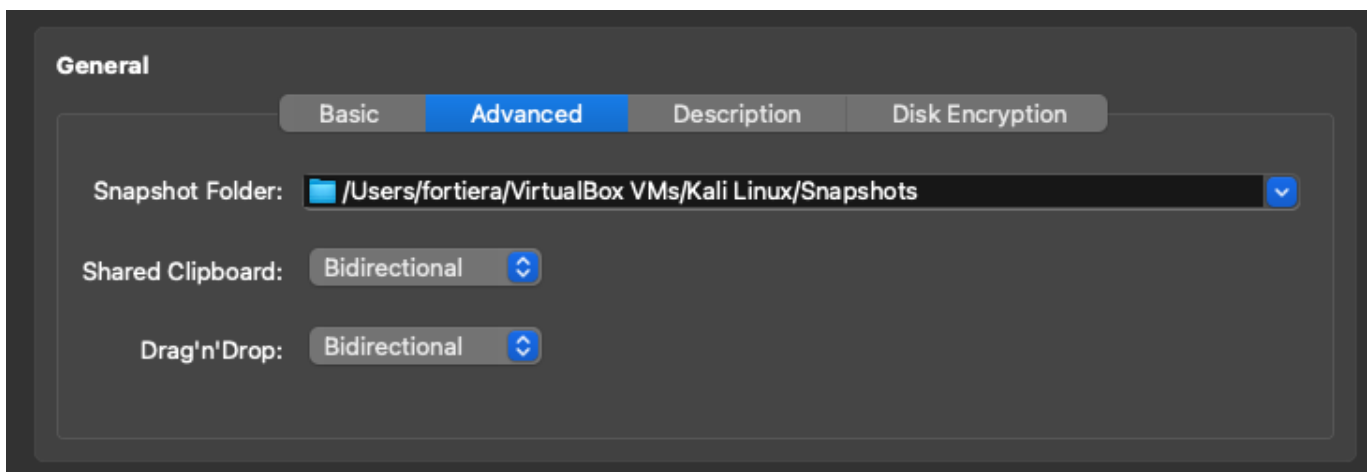
! chane **warnaud** by the name of your user

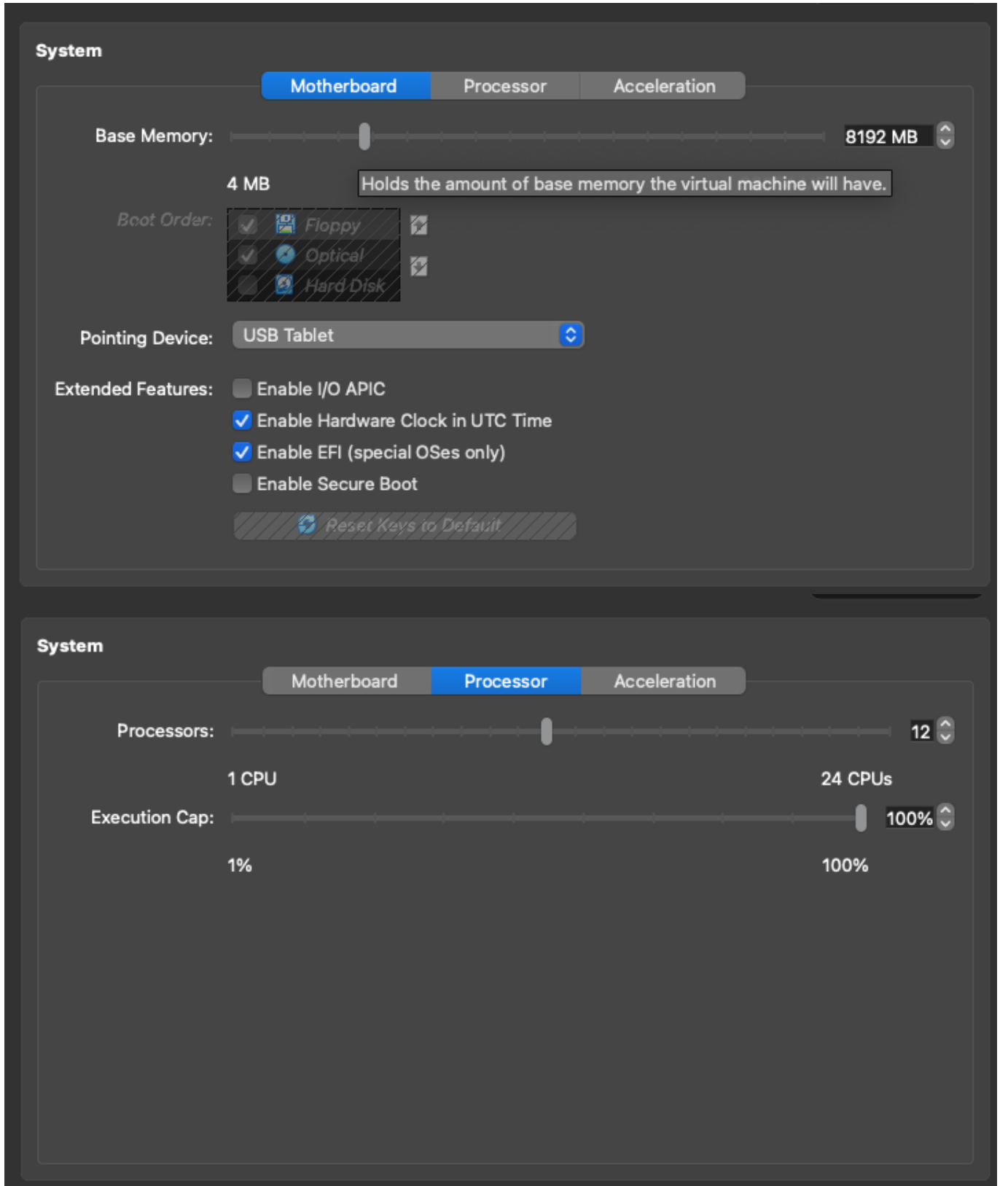


Fine tuning

stop the machine and click on the settings button to fine tune it:

- add more RAM and CPU if possible (runs fine with defaults)
- add clipboard
- 3D acceleration
- disable audio
- share folder





Display

Screen Remote Display Recording

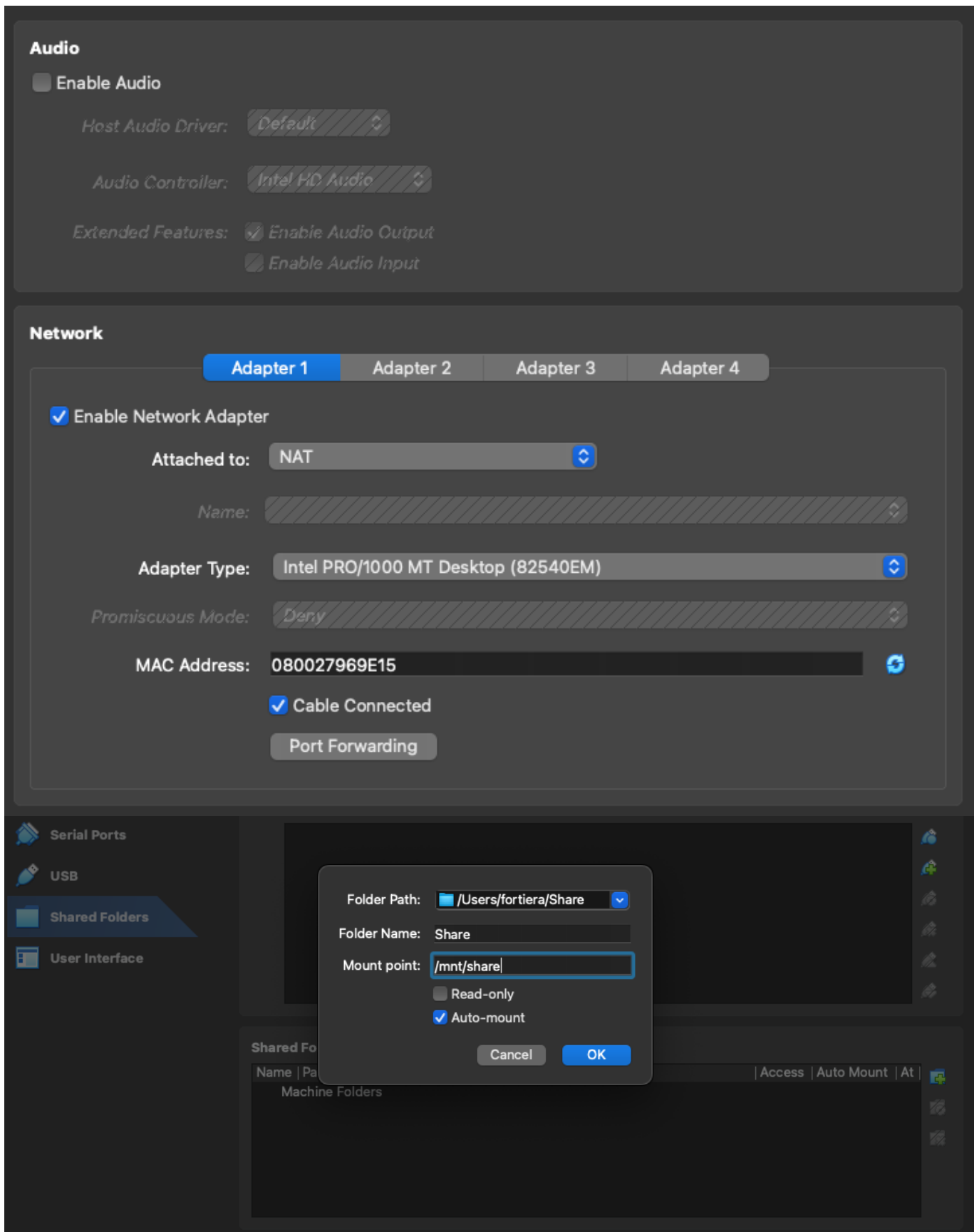
Video Memory: 0 MB 128 MB 128 MB

Monitor Count: 1 8

Scale Factor: All Monitors 100% 300% 100%

Graphics Controller: VMSVGA

Extended Features: Enable 3D Acceleration



Extra packages

Start the machine, now you "should be able to copy/paste commands !

```
apt update && apt install -y htop ccze dfc iftop libreoffice libreoffice-
```

```
ll0n-de libreoffice-ll0n-fr clipit zaproxy
```

Hacks

sudoers

```
sudo su
```

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

Autologin

```
sudo su
```

Manual

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

```
...  
[Seat:*]  
...  
autologin-user=kali  
autologin-user-timeout=0  
...
```

One-liner



```
sudo sed -i 's/#autologin-user=/autologin-user=kali/g; s/#autologin-user-timeout=0/autologin-user-timeout=0/g' /etc/lightdm/lightdm.conf
```

Extra packages

Docker

```
sudo su
```

```
apt update  
apt install -y apt-transport-https ca-certificates curl gnupg lsb-release  
# Add Docker's official GPG key
```

```
curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
# Add Docker repository (using Debian as base since Kali is Debian-based)
echo "deb [arch=arm64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian bullseye stable" | tee /etc/apt/sources.list.d/docker.list > /dev/null

# Update package list again
apt update
apt install -y docker-ce docker-ce-cli containerd.io
systemctl enable docker --now
usermod -aG docker kali
```

Docker-compose

check: <https://github.com/docker/compose/releases/> for url

```
sudo su
```

```
sudo wget https://github.com/docker/compose/releases/download/v2.30.3/docker-compose-linux-aarch64 -O /usr/bin/docker-compose
chmod +x /usr/bin/docker-compose
```

Test

Does it work?



log out or reboot so the user kali is part of the docker group



```
docker info
docker-compose info
```

Volatility 2 & python2

```
sudo su
```

```
# Install dependencies
apt install -y python2 python2-dev build-essential git libdistorm3-dev yara libraw1394-11 libcapstone-dev capstone-tool tzdata libpython2-dev libjpeg-dev zlib1g-dev libfreetype6-dev liblcms2-dev libwebp-dev tcl8.6-dev tk8.6-dev python2.7-tk
#Install pip
cd
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
python2 get-pip.py
# Install Python deps with python2 pip
```

```
python2 -m pip install -U setuptools wheel
python2 -m pip install importlib
python2 -m pip install distorm3
python2 -m pip install pycrypto
python2 -m pip install yara-python==3.11.0
python2 -m pip install pillow
python2 -m pip install openpyxl
python2 -m pip install pytz
python2 -m pip install ipython
python2 -m pip install capstone
# link yara
ln -s /usr/lib/aarch64-linux-gnu/libyara.so.10 /usr/lib/libyara.so
# Check python & yara are working
python2 -c "import yara; print('YARA Python working')"
yara --version

# Clone Volatility 2
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
```

Volatility 3

```
sudo su
```

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

Yara

```
sudo su
```

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

From:

<https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link:

<https://wiki.fortier-family.com/os/kali/css-arm>

Last update: 2024/11/16 15:16

