How to securely isolate Kali Linux with VirtualBox

Motivation

Similar to my paper, How to securely isolate Damn Vulnerable Linux with VirtualBox, this paper takes the next step at installing Kali Linux. I cannot speak highly enough of Kali Linux. Here is a list of the tools that come with Kali:

http://tools.kali.org/tools-listing

My goal is to write about as many of the tools, and what I find with those tools as time permits.
To re-iterate, the key with this lab is running all of the virtual machines inside of VirtualBox with their network adapters set to Host-only. This allows safe handling (isolation) of systems that could otherwise be exploited and leveraged as jump points into your corporate or home infrastructure.

Test environment layout

My workstation is running Ubuntu 16.10.
I am first installing VirtualBox 5.1.6 for Ubuntu, using method 2 below.
Then Kali Linux.

Install VirtualBox

Method 1:

Download software package from:

https://www.virtualbox.org/wiki/Linux_Downloads

```
$ cd ~/Downloads
$ wget http://download.virtualbox.org/virtualbox/5.1.10/virtualbox-
5.1_5.1.10-112026~Ubuntu~yakkety_amd64.deb
$ sudo dpkg -i virtualbox-5.1_5.1.10-112026-Ubuntu-yakkety_amd64.deb
```

Method 2:

Append the following line to your /etc/apt/sources.list (assuming it doesn't exist):

```
deb http://download.virtualbox.org/virtualbox/debian yakkety contrib
```

From Terminal (the $ means you are running this from your regular user account):

```
$ cd ~/Downloads
$ wget https://www.virtualbox.org/download/oracle_vbox_2016.asc
$ wget https://www.virtualbox.org/download/oracle_vbox.asc
$ sudo apt-key add oracle_vbox_2016.asc
$ sudo apt-key add oracle_vbox.asc
$ sudo apt-get update
$ sudo apt-get install virtualbox
$ sudo apt-get install dkms
$ sudo apt install virtualbox-ext-pack
$ sudo apt-get install virtualbox-ext-pack virtualbox-guest-additions-iso
```

Either method will work, I prefer method 2 because then you can get updates with the software.

Configure the multiple network domains:

This assumes you have not done this or need to modify your network.

Create NAT'ed Network:

When you see the “# at the beginning of a command line, that means you are running as root.

```
# VBoxManage natnetwork add \
  --netname 192.168.139-NAT \
  --network "192.168.139.0/24" \
  --enable --dhcp on
```

Create the DHCP server:

```
# VBoxManage dhcpserver add \
  --netname 192.168.139-NAT \
  --ip 192.168.139.3 \
  --lowerip 192.168.139.101 \
  --upperip 192.168.139.254 \
  --netmask 255.255.255.0 \
  --enable
```

Create hostonly interface:

```
# VBoxManage hostonlyif create
# VBoxManage hostonlyif ipconfig vboxnet0 \
  --ip 172.20.0.1 \
  --netmask 255.255.255.0
# VBoxManage dhcpserver add \
  --ifname vboxnet0 \
  --ip 172.20.0.3 \
  --lowerip 172.20.0.101 \
  --upperip 172.20.0.254 \
  --netmask 255.255.255.0
# VBoxManage dhcpserver modify \
  --ifname vboxnet0 \
  --enable
```

To list the NAT'ed networks:

```
# VBoxManage list natnetworks
```

Output:

```
NetworkName:    192.168.139-NAT
IP:             192.168.139.1
Network:        192.168.139.0/24
IPv6 Enabled:   No
IPv6 Prefix:    fd17:625c:f037:a88b::/64
DHCP Enabled:   Yes
Enabled:        Yes
loopback mappings (ipv4)
        127.0.0.1=2
```

To List the DHCP server(s):

```
# VBoxManage list dhcpservers
```

Output:

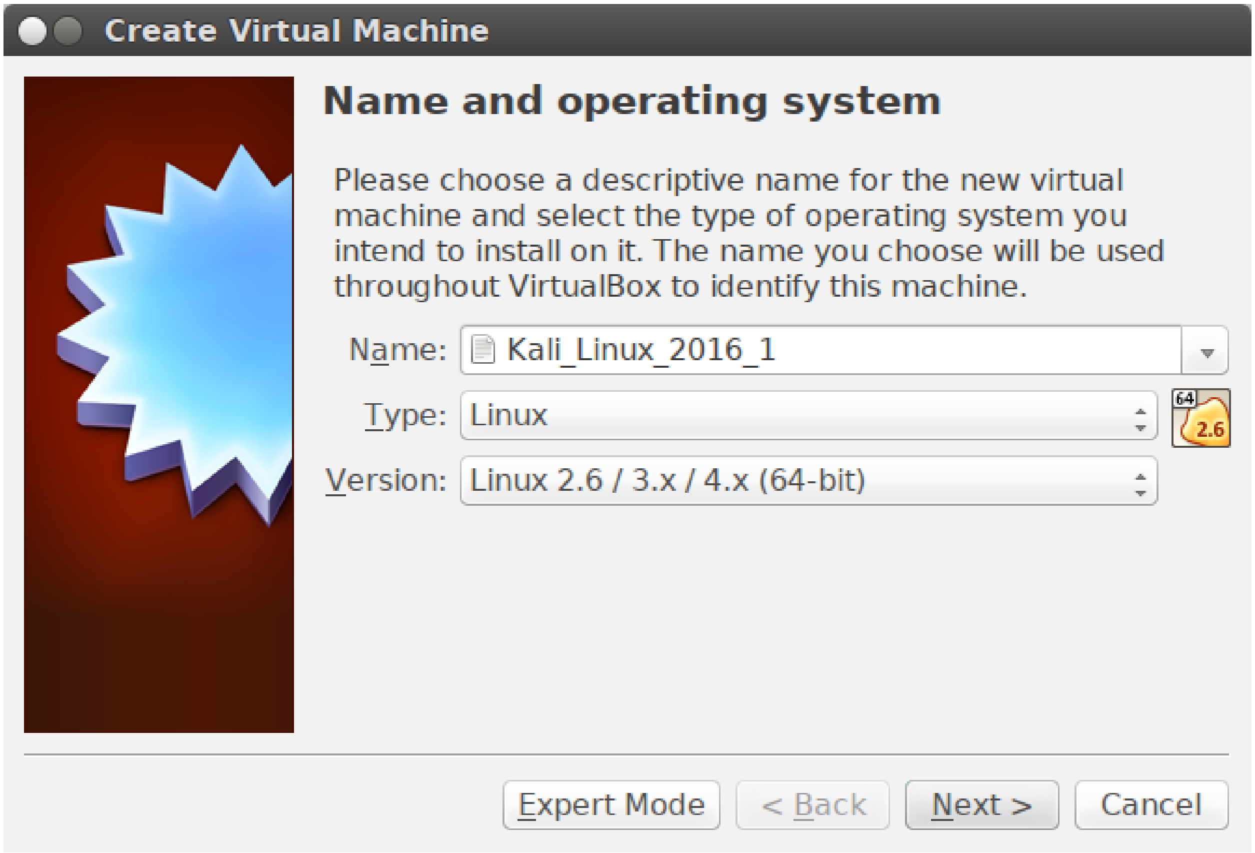
```
NetworkName:    192.168.139-NAT
IP:             192.168.139.3
NetworkMask:    255.255.255.0
lowerIPAddress: 192.168.139.101
upperIPAddress: 192.168.139.254
Enabled:        Yes

NetworkName:    HostInterfaceNetworking-vboxnet0
IP:             172.20.0.3
NetworkMask:    255.255.255.0
lowerIPAddress: 172.20.0.101
upperIPAddress: 172.20.0.254
Enabled:        Yes

NetworkName:    HostInterfaceNetworking-vboxnet1
IP:             0.0.0.0
NetworkMask:    0.0.0.0
lowerIPAddress: 0.0.0.0
upperIPAddress: 0.0.0.0
Enabled:        No
```

Download the Official Release of Kali Linux

Get the ISO from here:

http://docs.kali.org/introduction/download-official-kali-linux-images

Setup new virtual machine for Kali Linux



Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Kali_Linux_2016_1

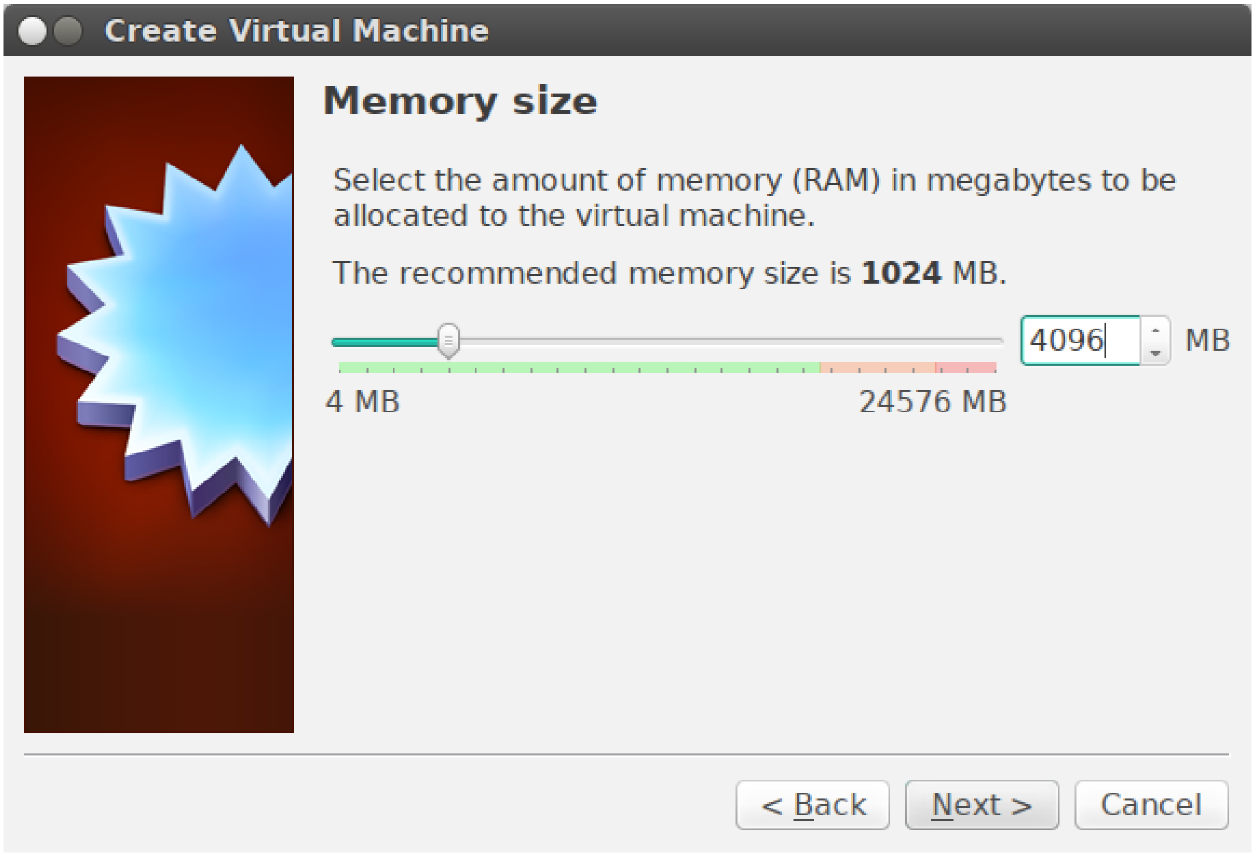
Type: Linux

Version: Linux 2.6 / 3.x / 4.x (64-bit)

Open VirtualBox and Click on New.

Give the virtual machine a name, choose Type Linux, Version: Linux 2.6 / 3.x / 4.x (64-bit).

Click Next.



Create Virtual Machine

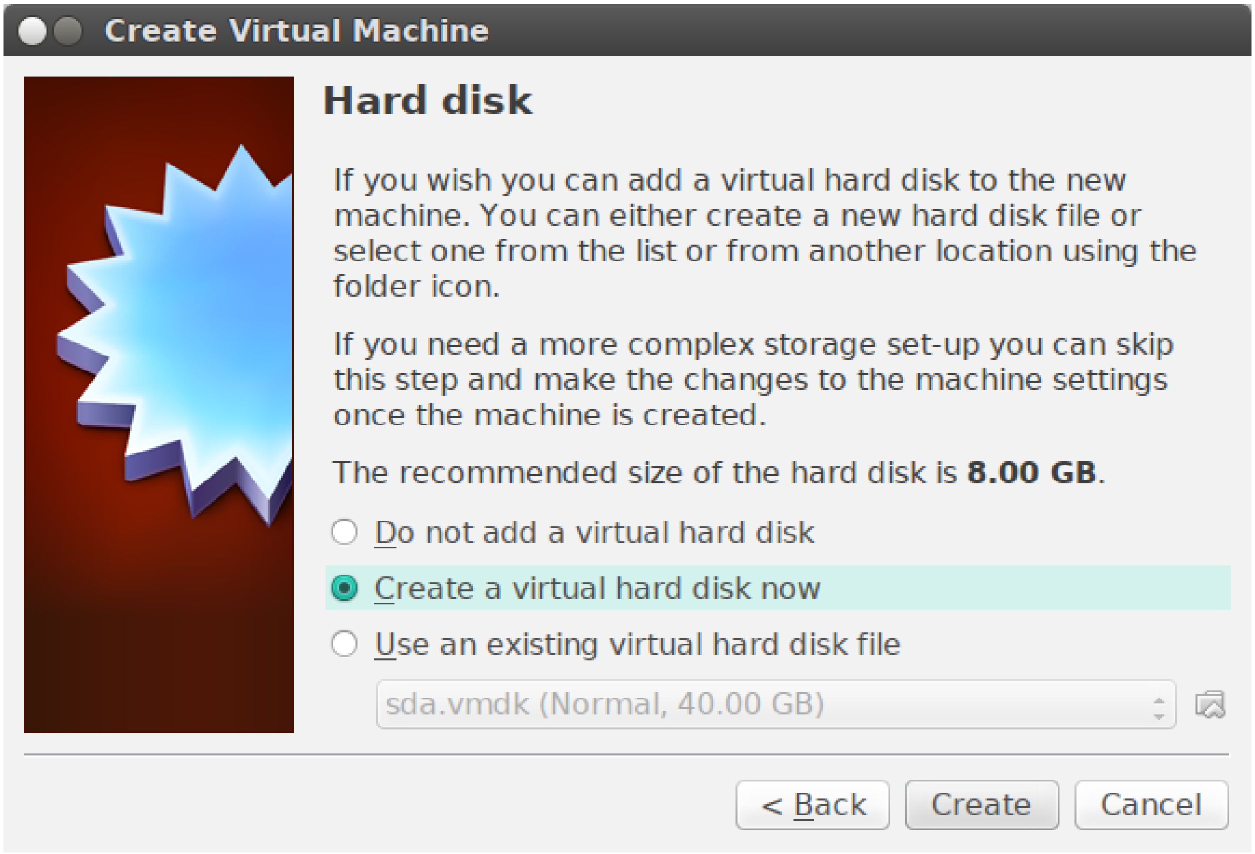
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

4096 MB

Set the Memory to 4GB and click on Next.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

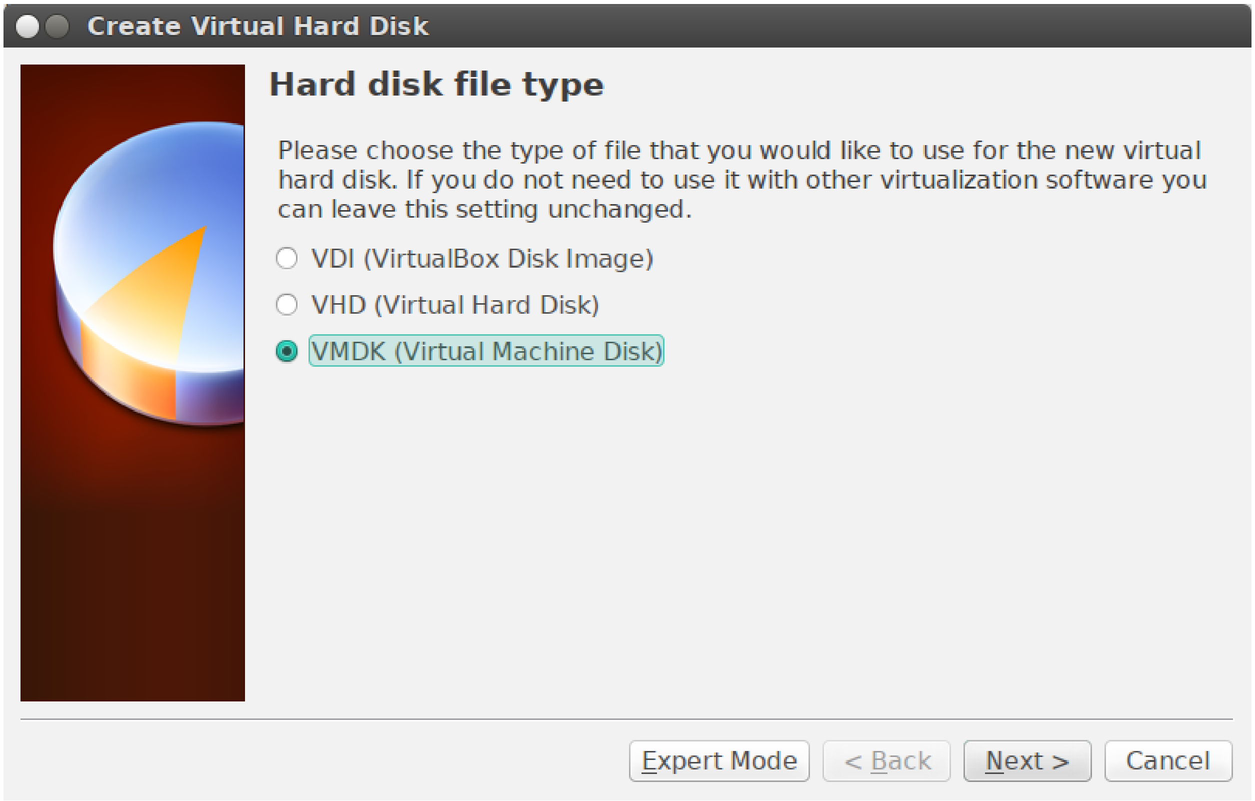
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

sda.vmdk (Normal, 40.00 GB)

Select the middle option and click Create.


Create Virtual Hard Disk

Hard disk file type

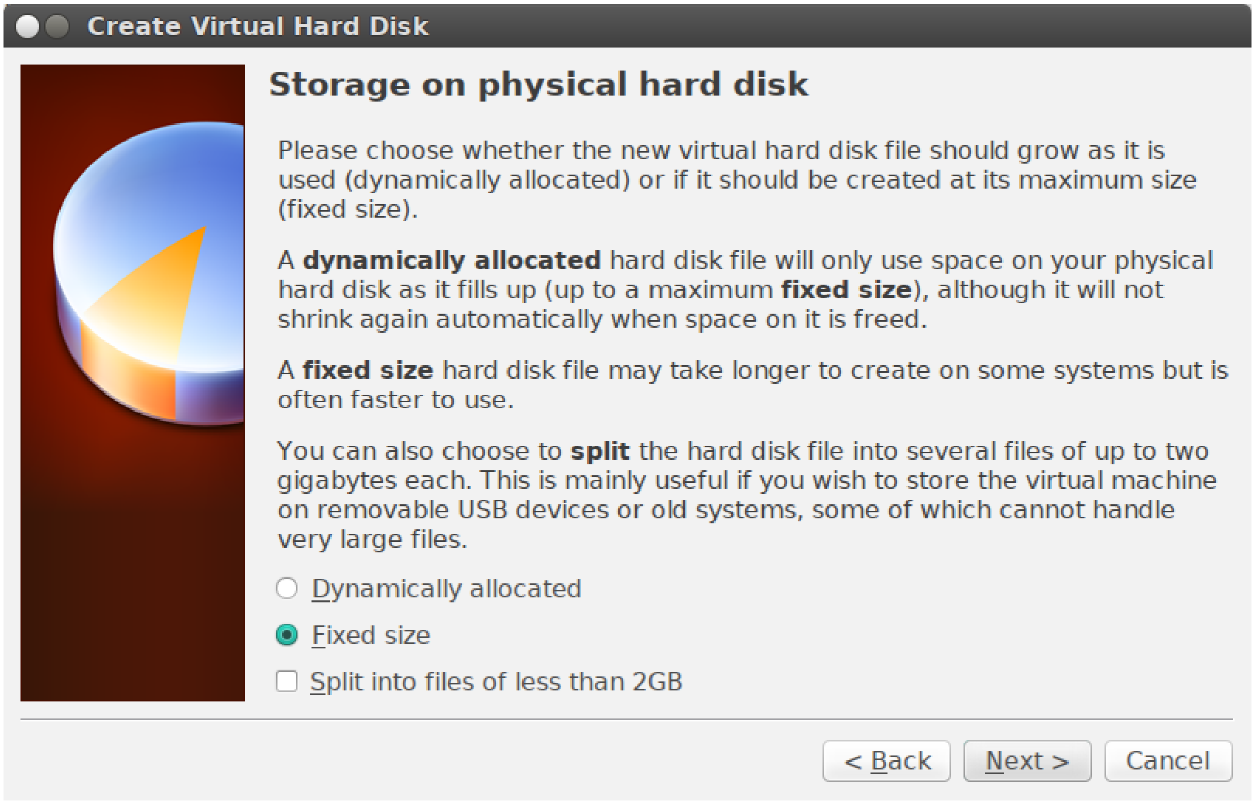
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

○ VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

● VMDK (Virtual Machine Disk)

Choose VMDK and click on Next.



Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

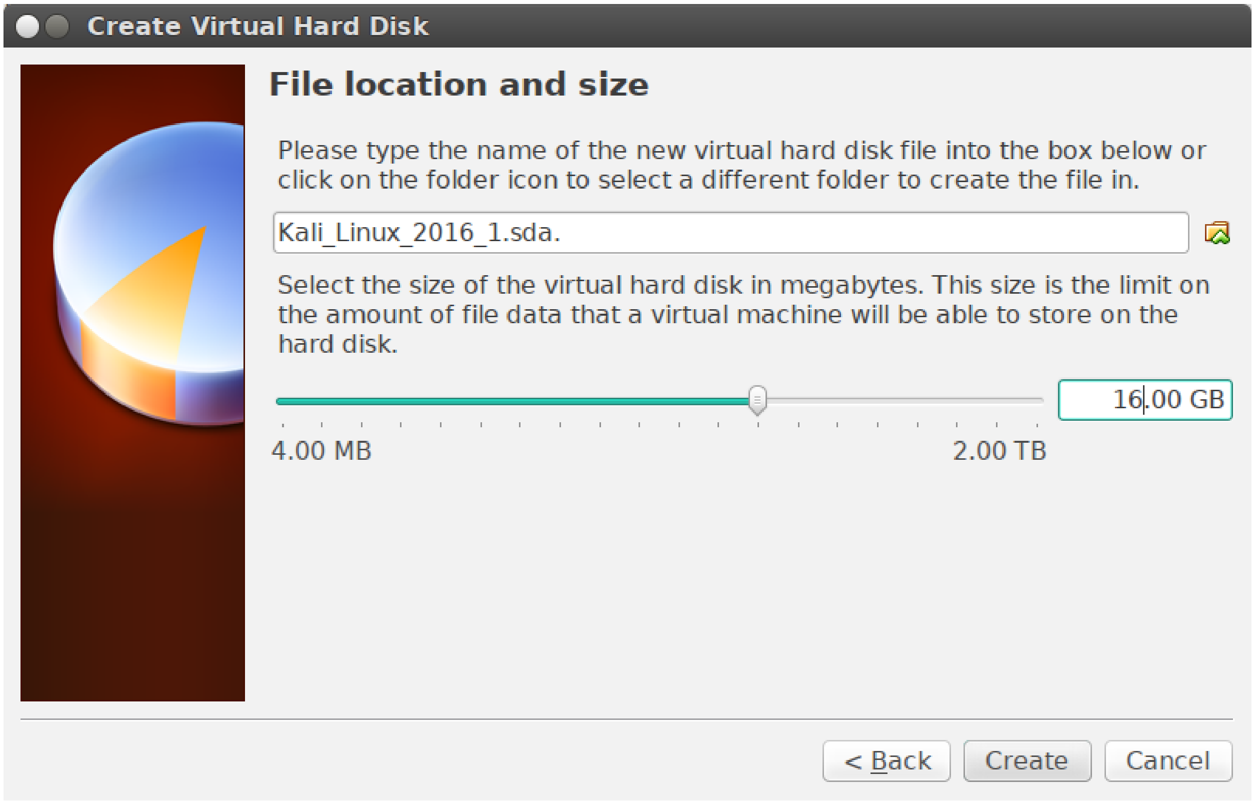
You can also choose to **split** the hard disk file into several files of up to two gigabytes each. This is mainly useful if you wish to store the virtual machine on removable USB devices or old systems, some of which cannot handle very large files.

○ Dynamically allocated

● Fixed size

□ Split into files of less than 2GB

Select Fixed Size and click on Next.



File location and size

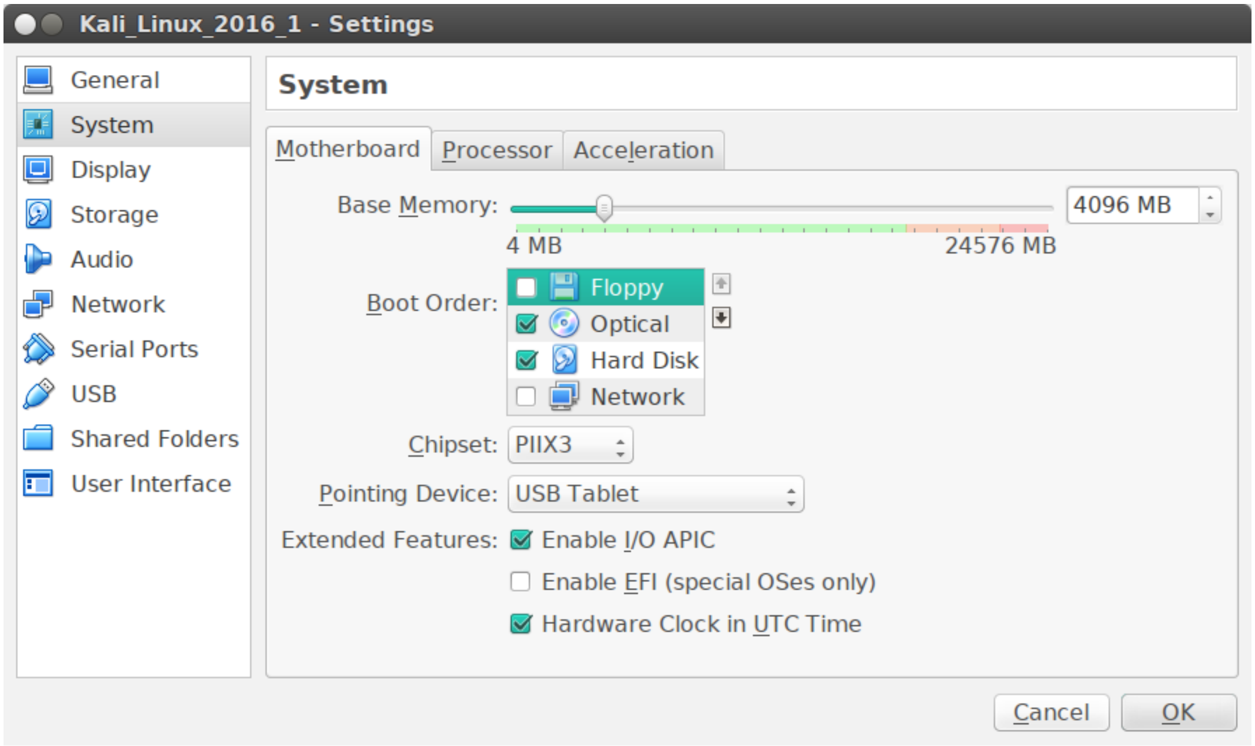
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

Kali_Linux_2016_1.sda.

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

16.00 GB

Label the disk “Kali_Linux_2016_1.sda and give it a size of 16 GB. Click on Create.



Kali_Linux_2016_1 - Settings

System

Base Memory: 4096 MB

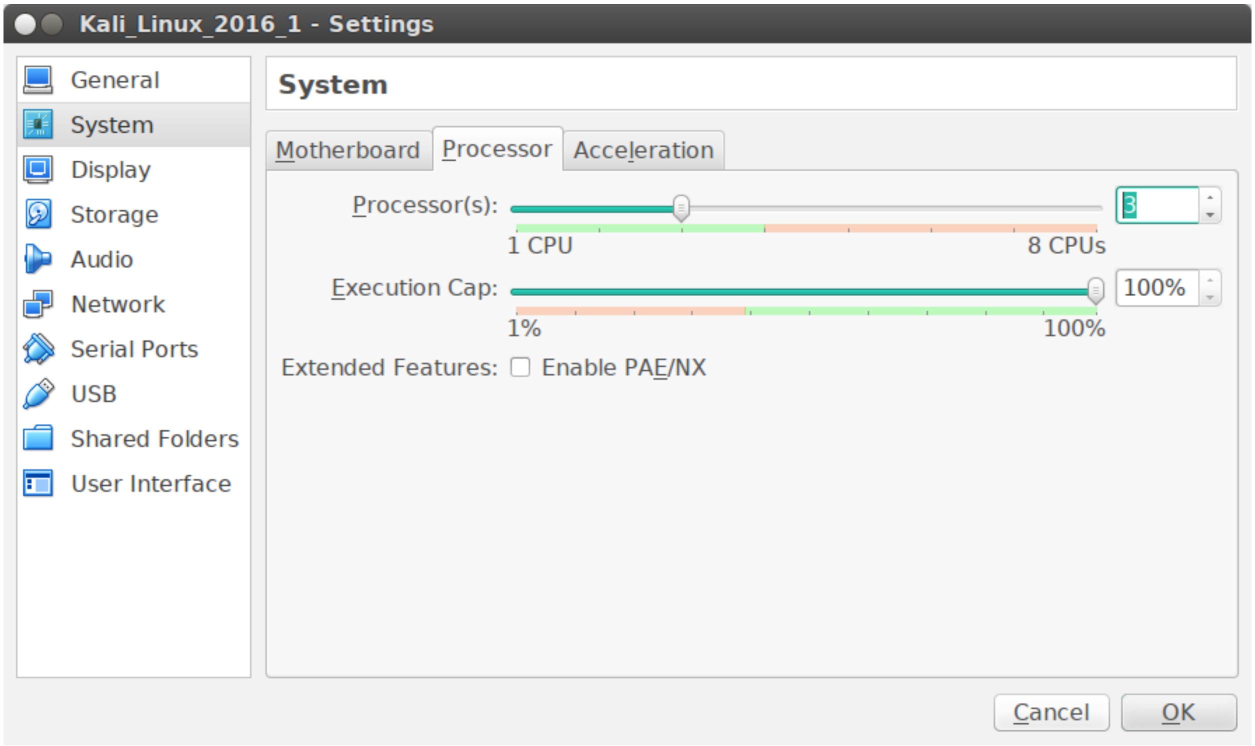
Boot Order:
☐ Floppy
☑ Optical
☑ Hard Disk
☐ Network

Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features:
☑ Enable I/O APIC
☐ Enable EFI (special OSes only)
☑ Hardware Clock in UTC Time

Once the virtual machine is created, highlight it and select Settings. Uncheck Floppy.



Kali_Linux_2016_1 - Settings

System

Processor(s): 3

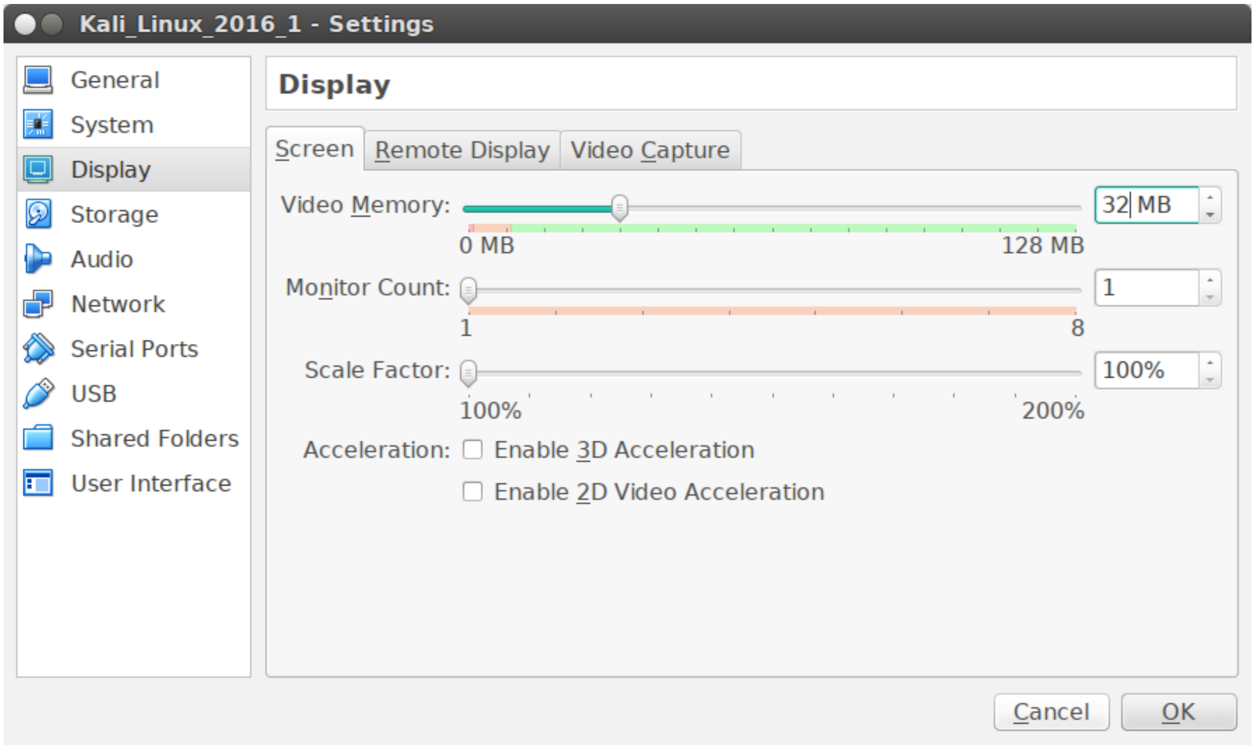
1 CPU 8 CPUs

Execution Cap: 100%

1% 100%

Extended Features: □ Enable PAE/NX

Change to 3 processors.



Kali_Linux_2016_1 - Settings

Display

Video Memory: 32 MB

0 MB 128 MB

Monitor Count: 1

1 8

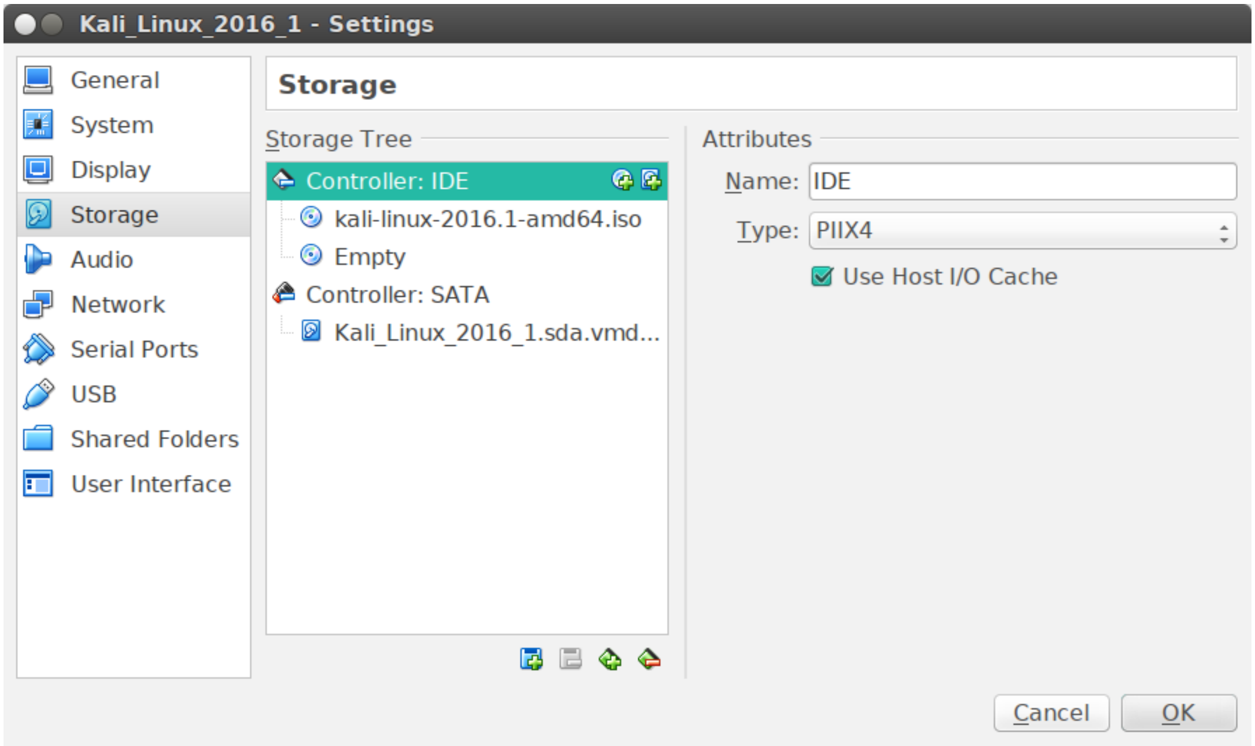
Scale Factor: 100%

100% 200%

Acceleration: □ Enable 3D Acceleration

□ Enable 2D Video Acceleration

Change the video memory from 16 to 32 MB.



Controller: IDE
- kali-linux-2016.1-amd64.iso
- Empty

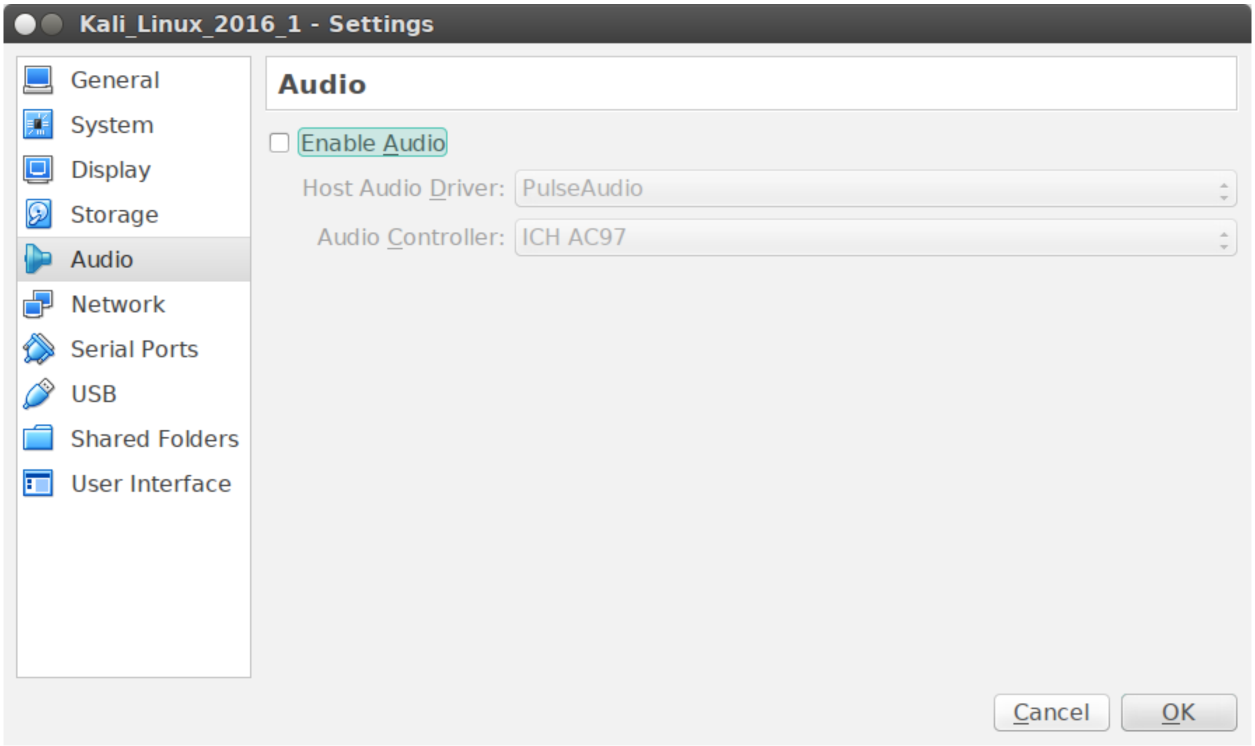
Controller: SATA
- Kali_Linux_2016_1.sda.vmd...

Name: IDE

Type: PIIX4

☑ Use Host I/O Cache

On Controller IDE, click on the plus sign above the CDROM icon, point to the Kali Linux ISO image.



Kali_Linux_2016_1 - Settings

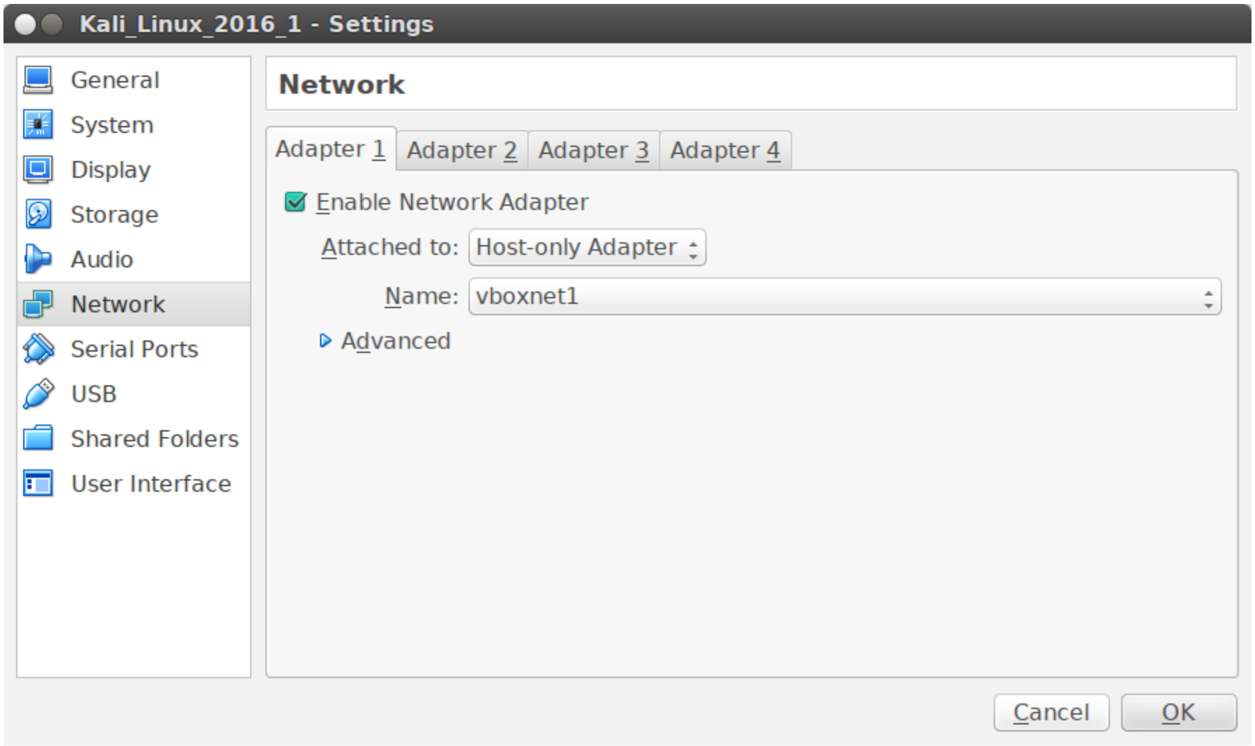
Audio

□ Enable Audio

Host Audio Driver: PulseAudio

Audio Controller: ICH AC97

Uncheck Enable Audio.



Kali_Linux_2016_1 - Settings

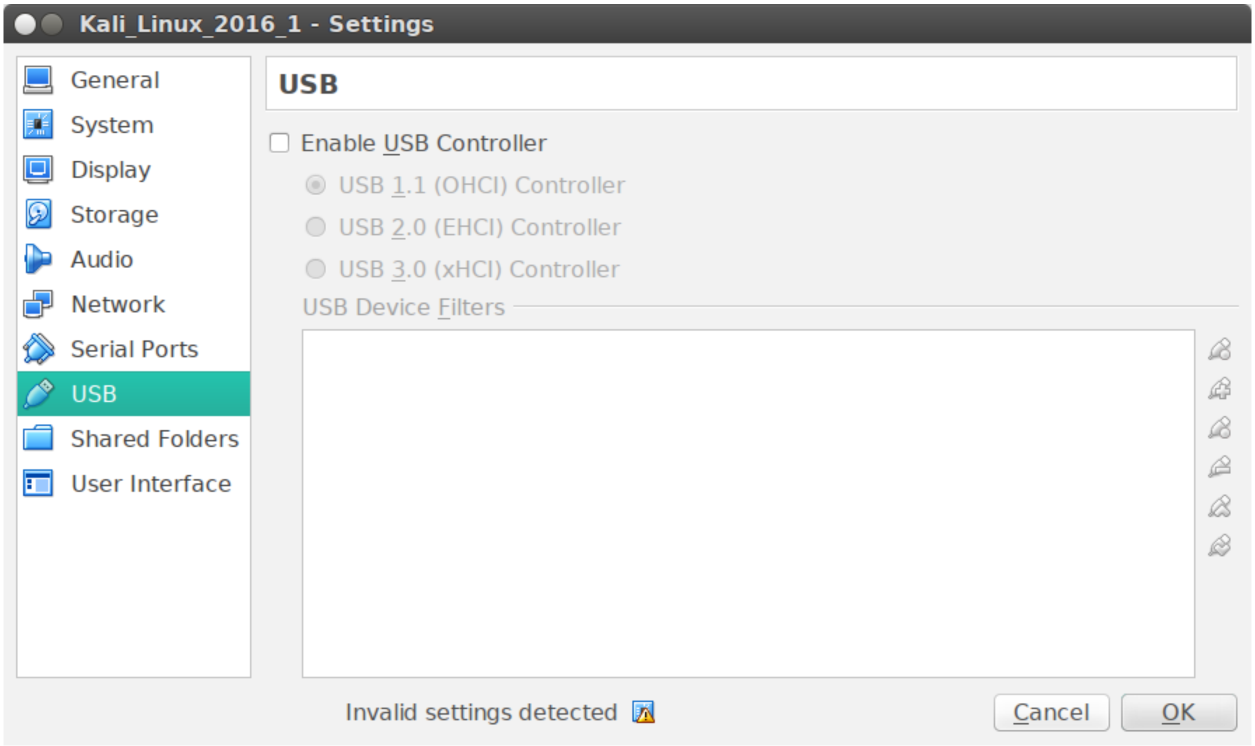
Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet1

Change the Adapter to Attached to: Host-only Adapter.



Kali_Linux_2016_1 - Settings

USB

☐ Enable USB Controller

● USB 1.1 (OHCI) Controller

○ USB 2.0 (EHCI) Controller

○ USB 3.0 (xHCI) Controller

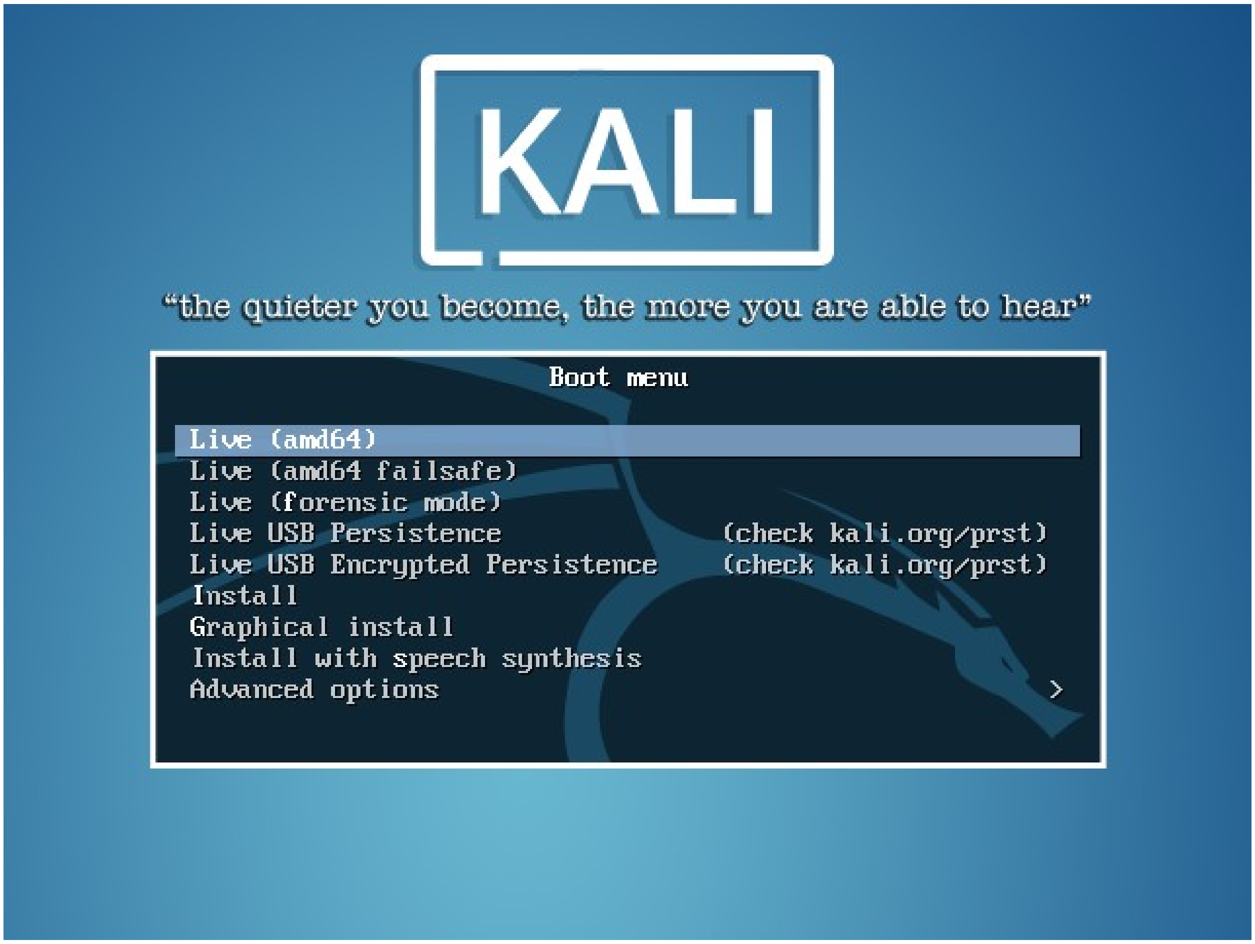
USB Device Filters

Invalid settings detected

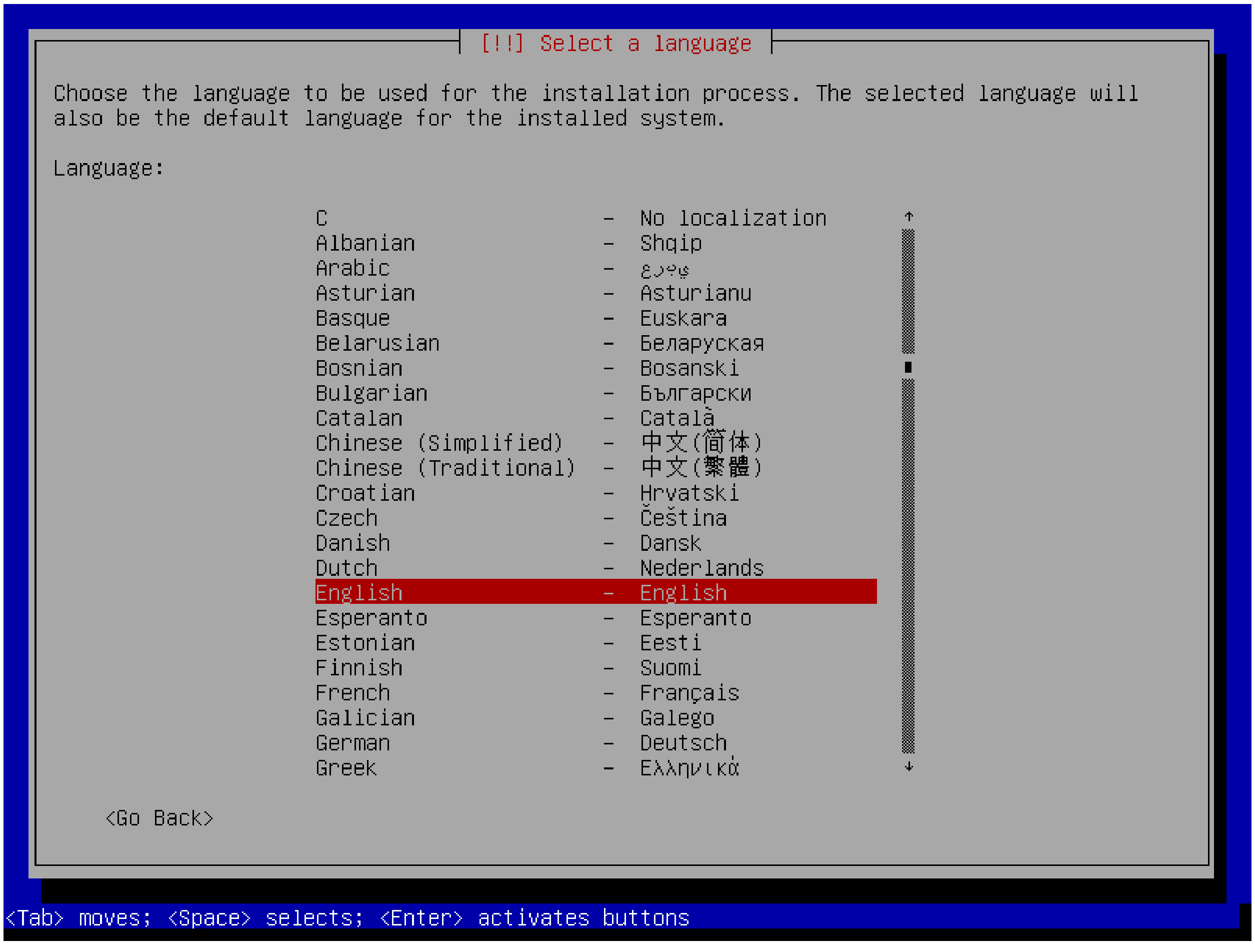
Finally, disable USB Controller. Click on OK to accept changes.

Start install process for Kali Linux

In VirtualBox, Highlight your virtual machine tilted, “Kali_Linux_2016_1” and click on the Start button.

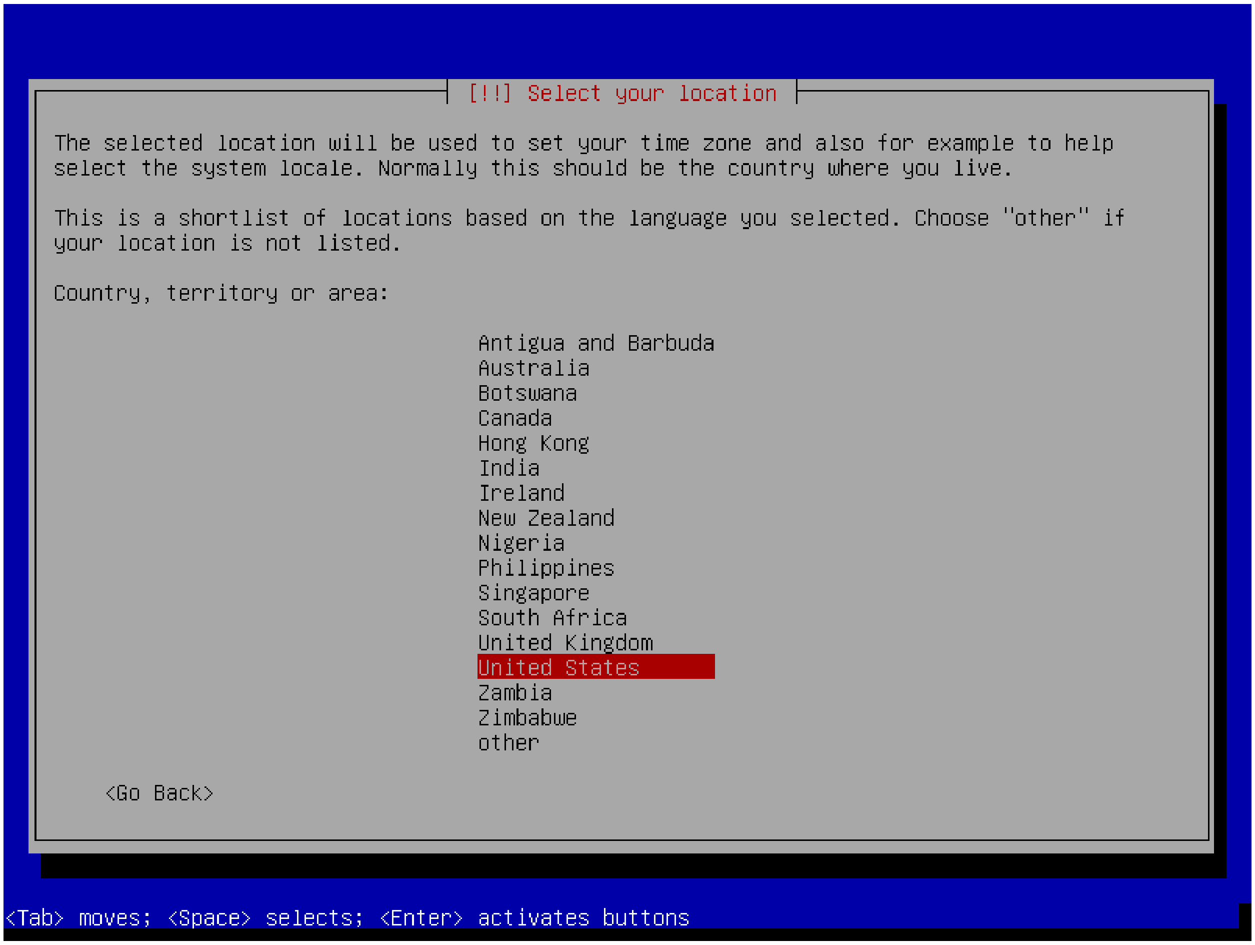

KALI
“the quieter you become, the more you are able to hear”
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options >

Scroll down to “Install” and press Enter.



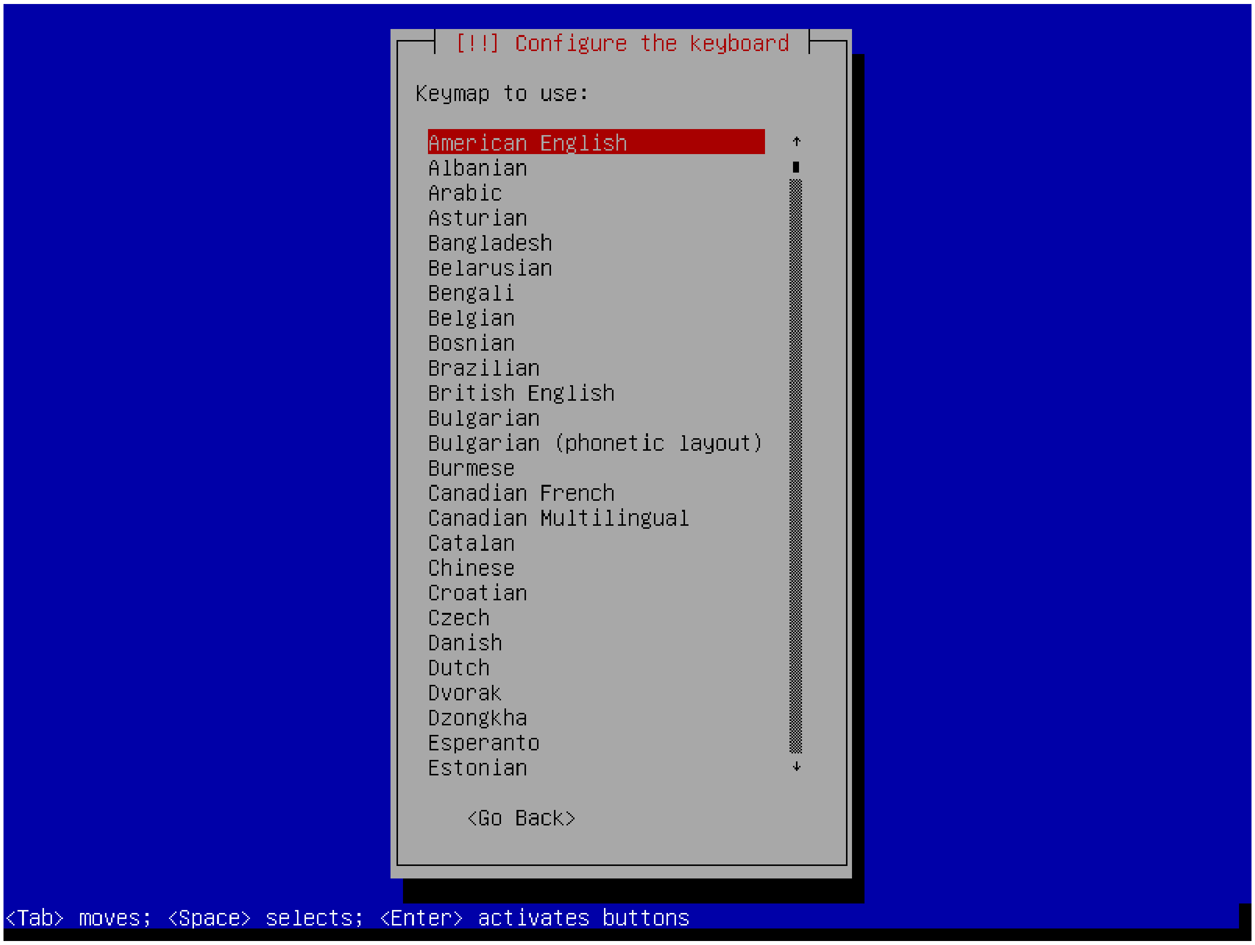
```
[!!] Select a language

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

Language:

                     C                       -  No localization
                     Albanian                -  Shqip
                     Arabic                  -  عربي
                     Asturian                -  Asturianu
                     Basque                  -  Euskara
                     Belarusian              -  Беларуская
                     Bosnian                 -  Bosanski
                     Bulgarian               -  Български
                     Catalan                 -  Català
                     Chinese (Simplified)    -  中文(简体)
                     Chinese (Traditional)   -  中文(繁體)
                     Croatian                -  Hrvatski
                     Czech                   -  Čeština
                     Danish                  -  Dansk
                     Dutch                   -  Nederlands
                     English                 -  English
                     Esperanto               -  Esperanto
                     Estonian                -  Eesti
                     Finnish                 -  Suomi
                     French                  -  Français
                     Galician                -  Galego
                     German                  -  Deutsch
                     Greek                   -  Ελληνικά

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Select your language and press Enter.



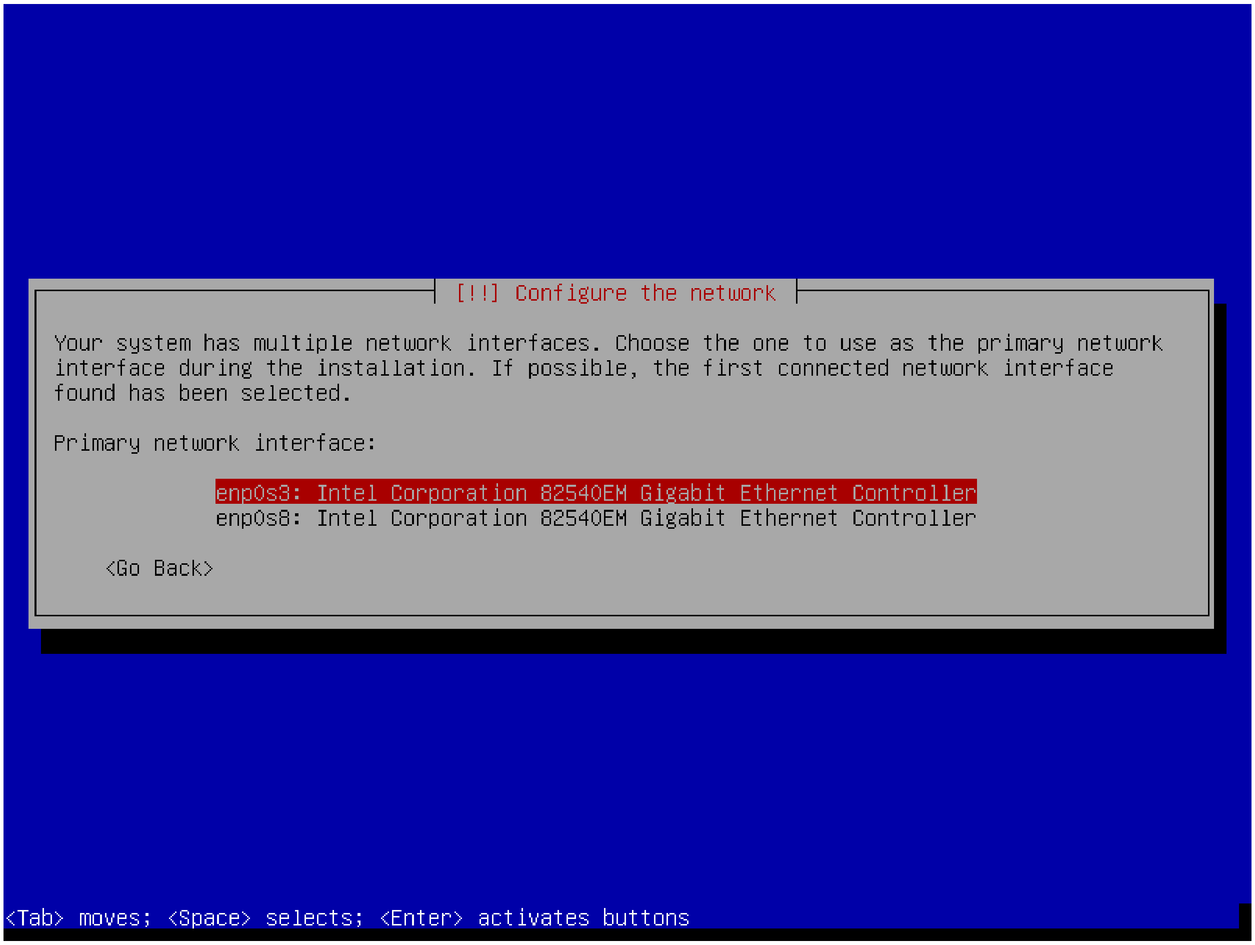
```
[!!] Select your location

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:

                                  Antigua and Barbuda
                                  Australia
                                  Botswana
                                  Canada
                                  Hong Kong
                                  India
                                  Ireland
                                  New Zealand
                                  Nigeria
                                  Philippines
                                  Singapore
                                  South Africa
                                  United Kingdom
                                  United States
                                  Zambia
                                  Zimbabwe
                                  other

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Choose your localle and hit Enter.



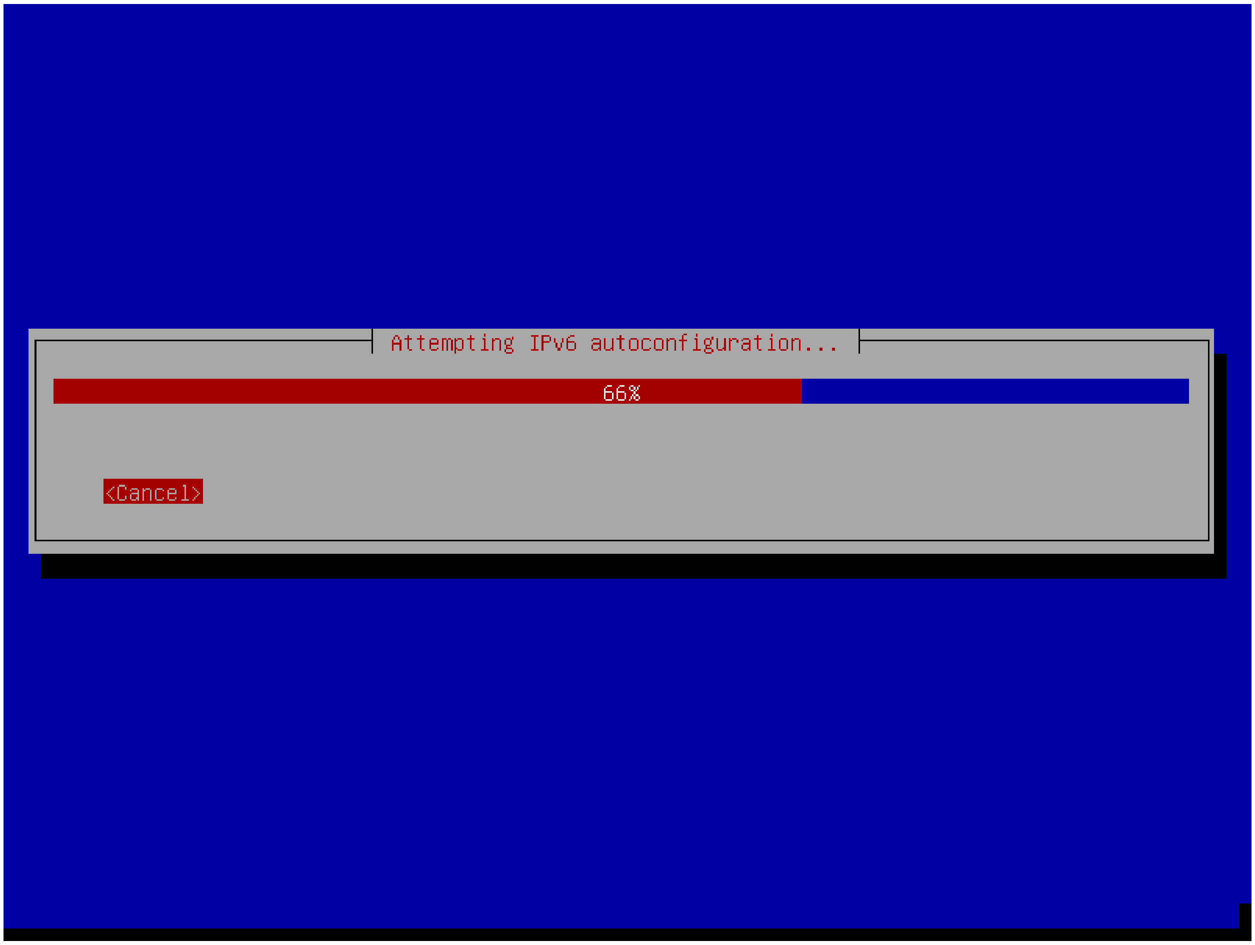
```
[!!] Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual
Catalan
Chinese
Croatian
Czech
Danish
Dutch
Dvorak
Dzongkha
Esperanto
Estonian

     <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Choose your keyboard and hit Enter.



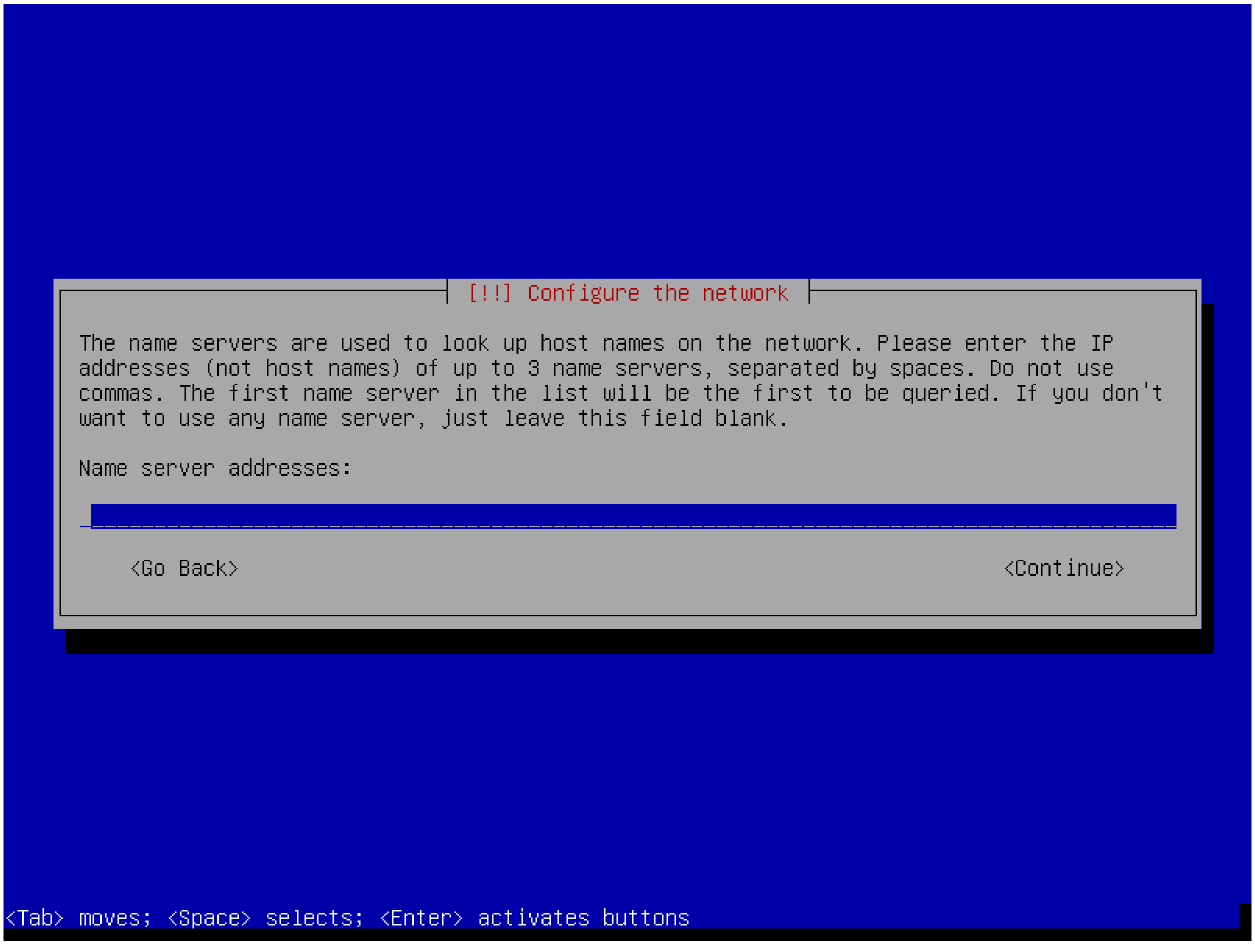
```
[!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network
interface during the installation. If possible, the first connected network interface
found has been selected.

Primary network interface:

             enp0s3: Intel Corporation 82540EM Gigabit Ethernet Controller
             enp0s8: Intel Corporation 82540EM Gigabit Ethernet Controller

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Choose your interface; it should be enp0s3 in this case. Hit Enter.



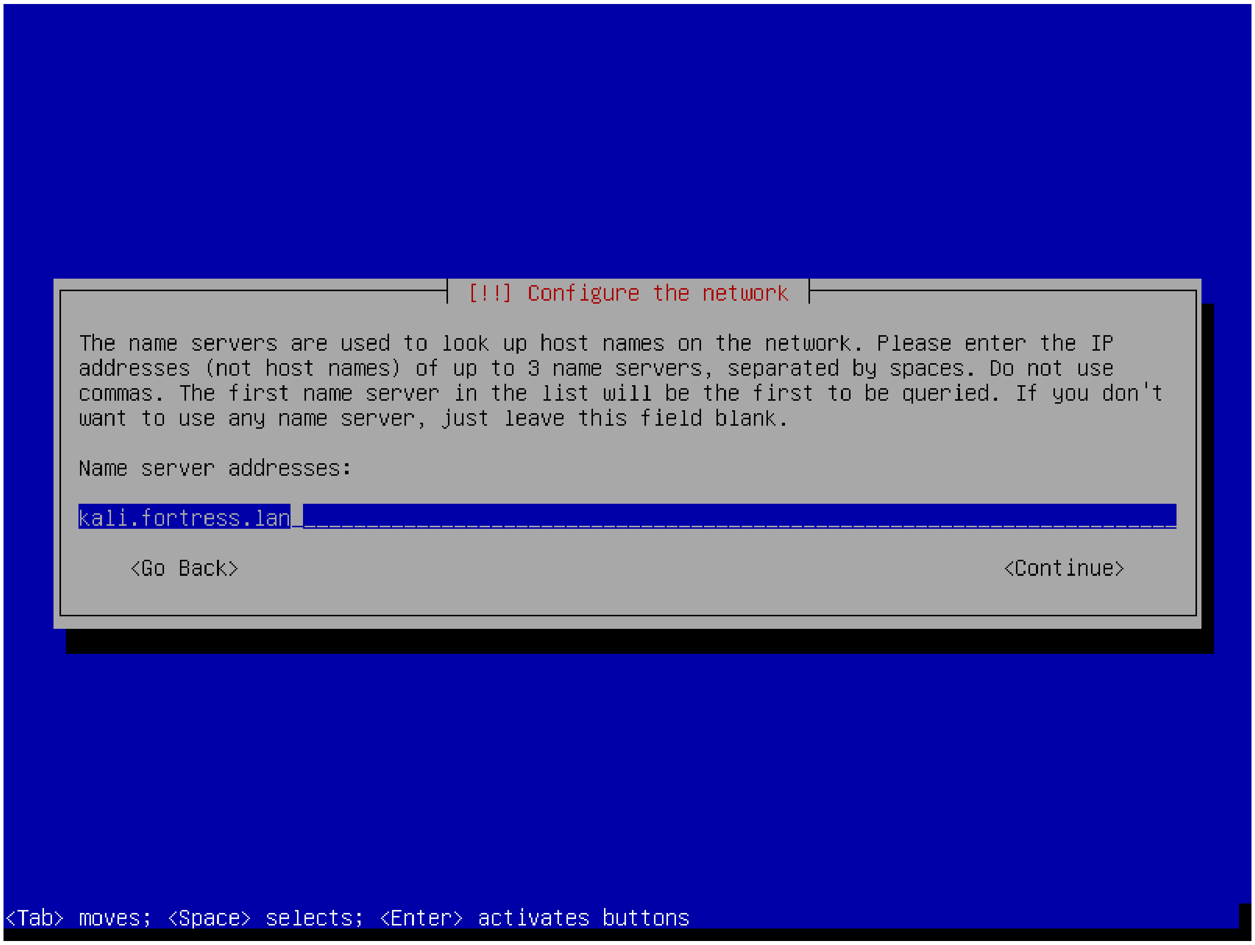
```
Attempting IPv6 autoconfiguration...

66%

<Cancel>
```

The system will start with trying to get a DHCP address. Wait.



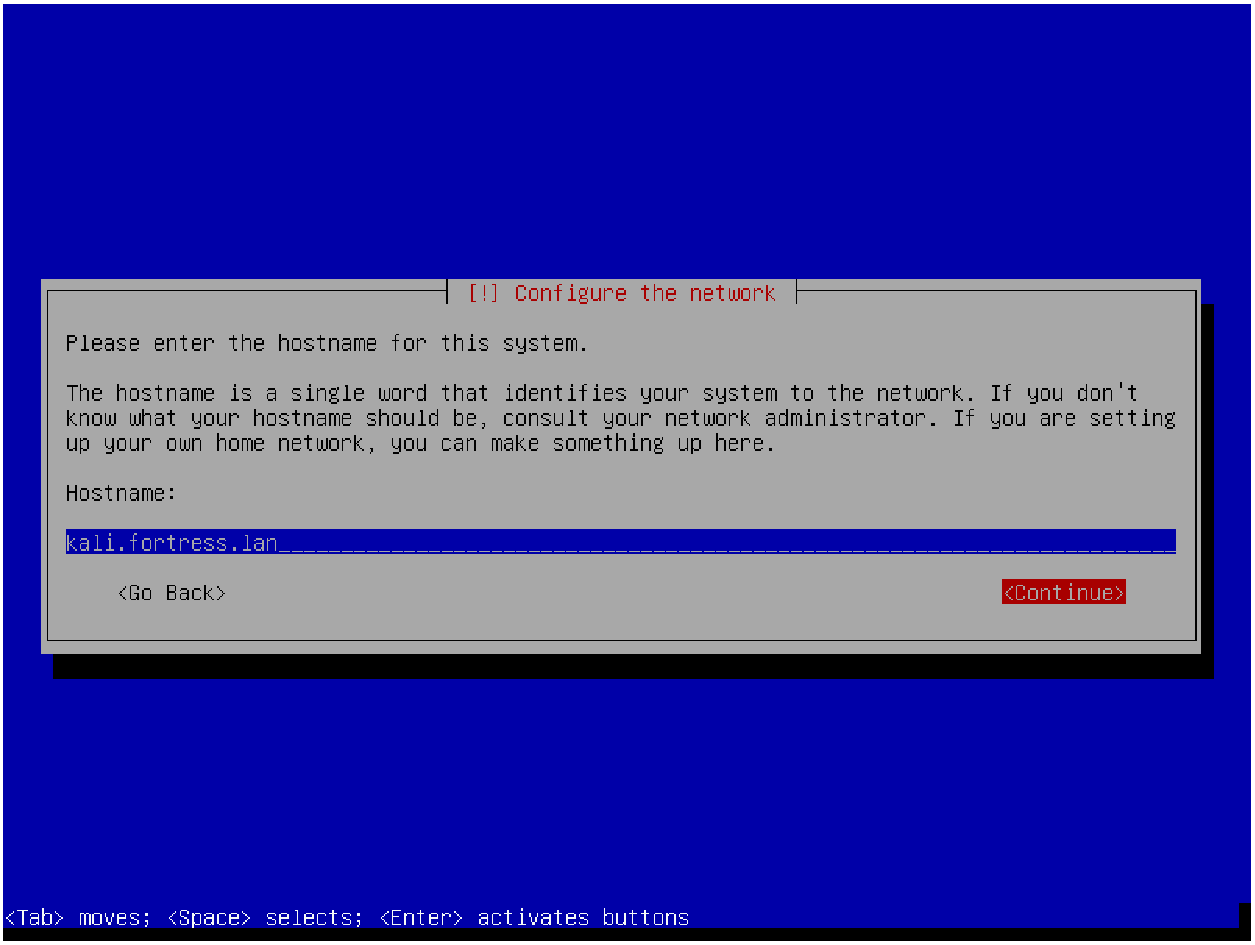
```
[!!] Configure the network

The name servers are used to look up host names on the network. Please enter the IP
addresses (not host names) of up to 3 name servers, separated by spaces. Do not use
commas. The first name server in the list will be the first to be queried. If you don't
want to use any name server, just leave this field blank.

Name server addresses:

_____________________________________________________________________________________

    <Go Back>                                                             <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Enter in a nameserver, e.g. 8.8.4.4 or 8.8.8.8. Tab to select Continue and press Enter.



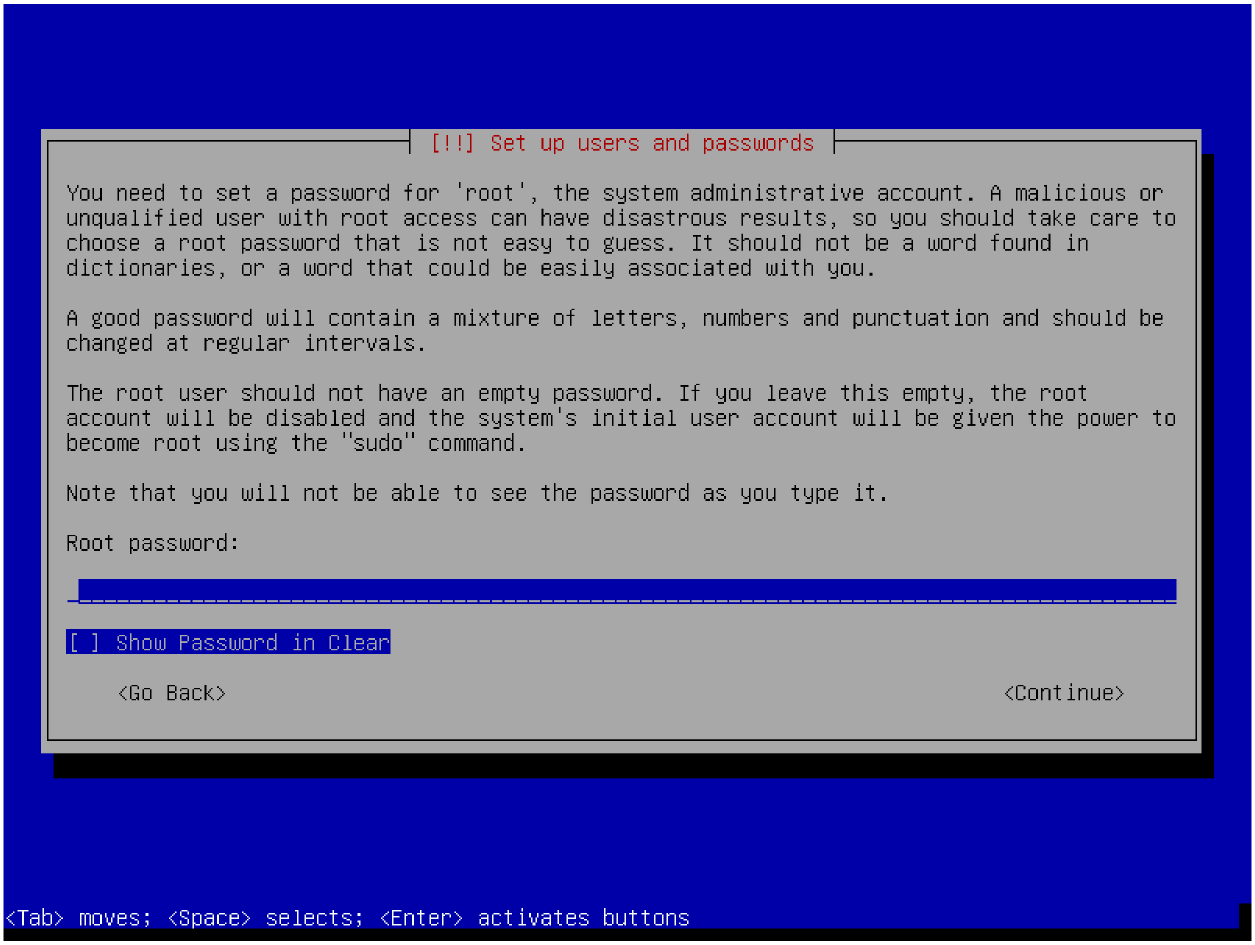
```
[!!] Configure the network

The name servers are used to look up host names on the network. Please enter the IP
addresses (not host names) of up to 3 name servers, separated by spaces. Do not use
commas. The first name server in the list will be the first to be queried. If you don't
want to use any name server, just leave this field blank.

Name server addresses:

kali.fortress.lan

<Go Back>                                                          <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Type in a hostname, tab to Continue and hit Enter.



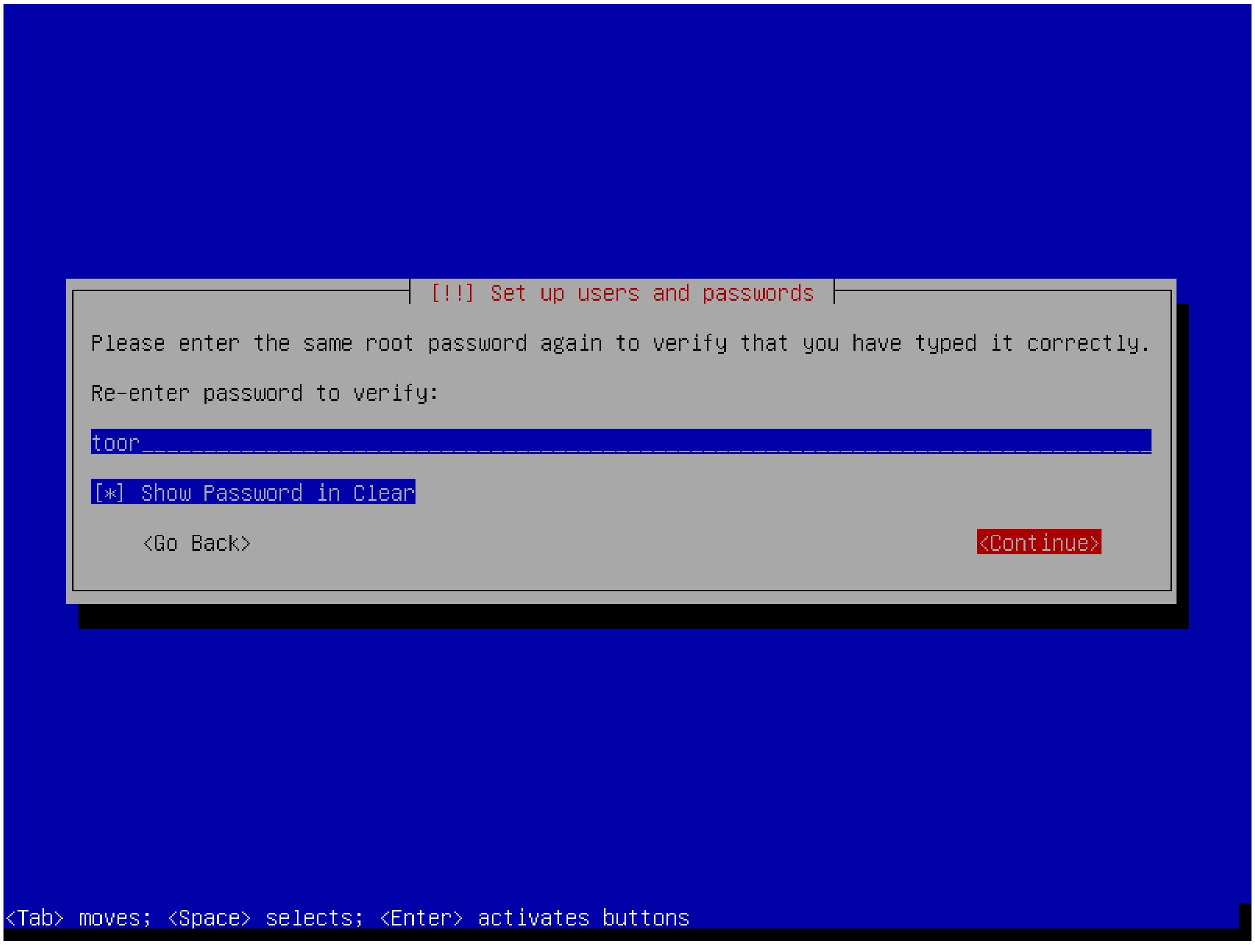
```
[!] Configure the network

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:

kali.fortress.lan_____________________________________________________________________

    <Go Back>                                                              <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Hit Enter.



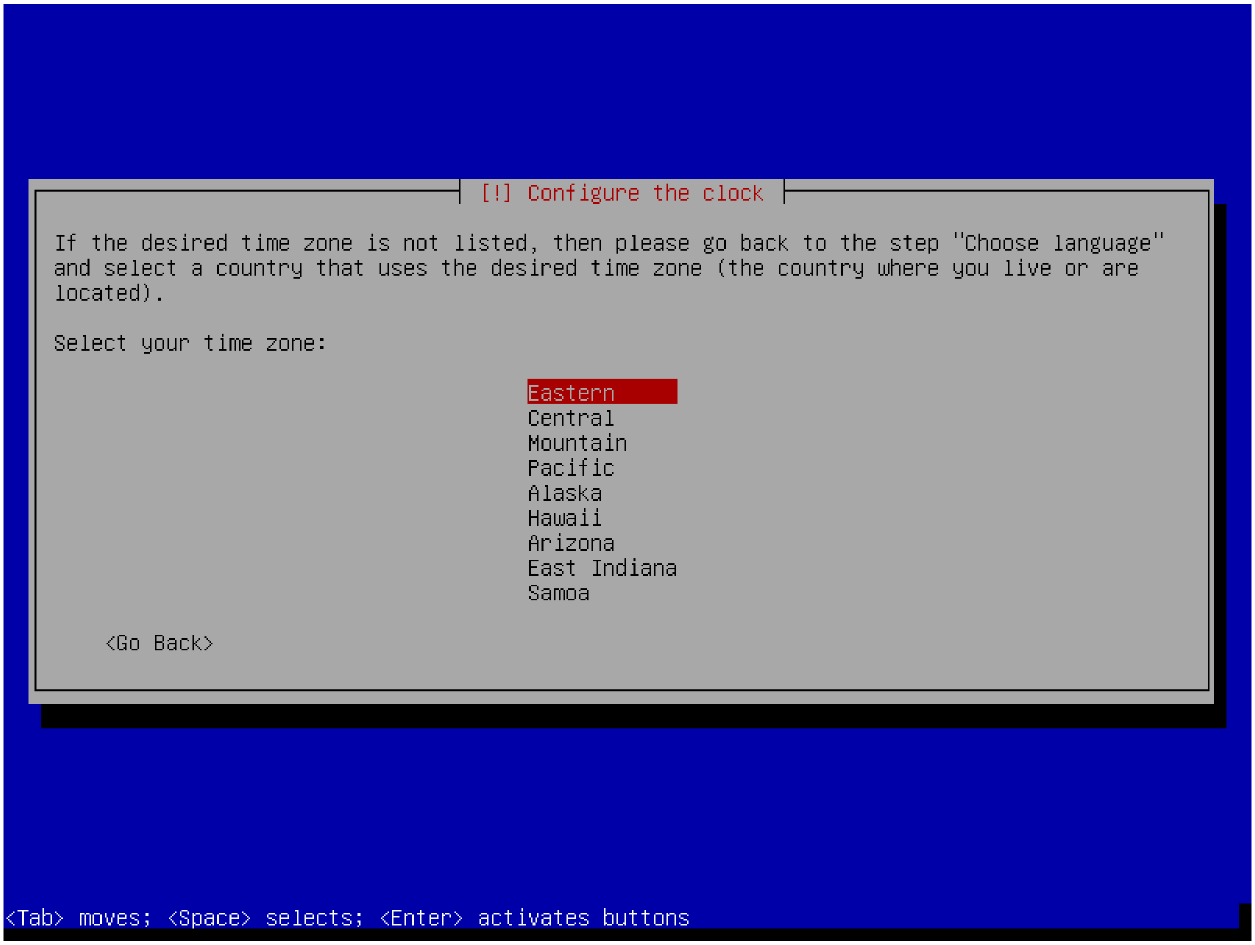
```
[!!] Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or
unqualified user with root access can have disastrous results, so you should take care to
choose a root password that is not easy to guess. It should not be a word found in
dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be
changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root
account will be disabled and the system's initial user account will be given the power to
become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

[ ] Show Password in Clear

    <Go Back>                                                            <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Enter in a root password, I chose “toor” to keep it consistent with the DVL instance. If someone hacks these instances, you’ve got bigger problems than a simple password. Tab to Continue and hit Enter.



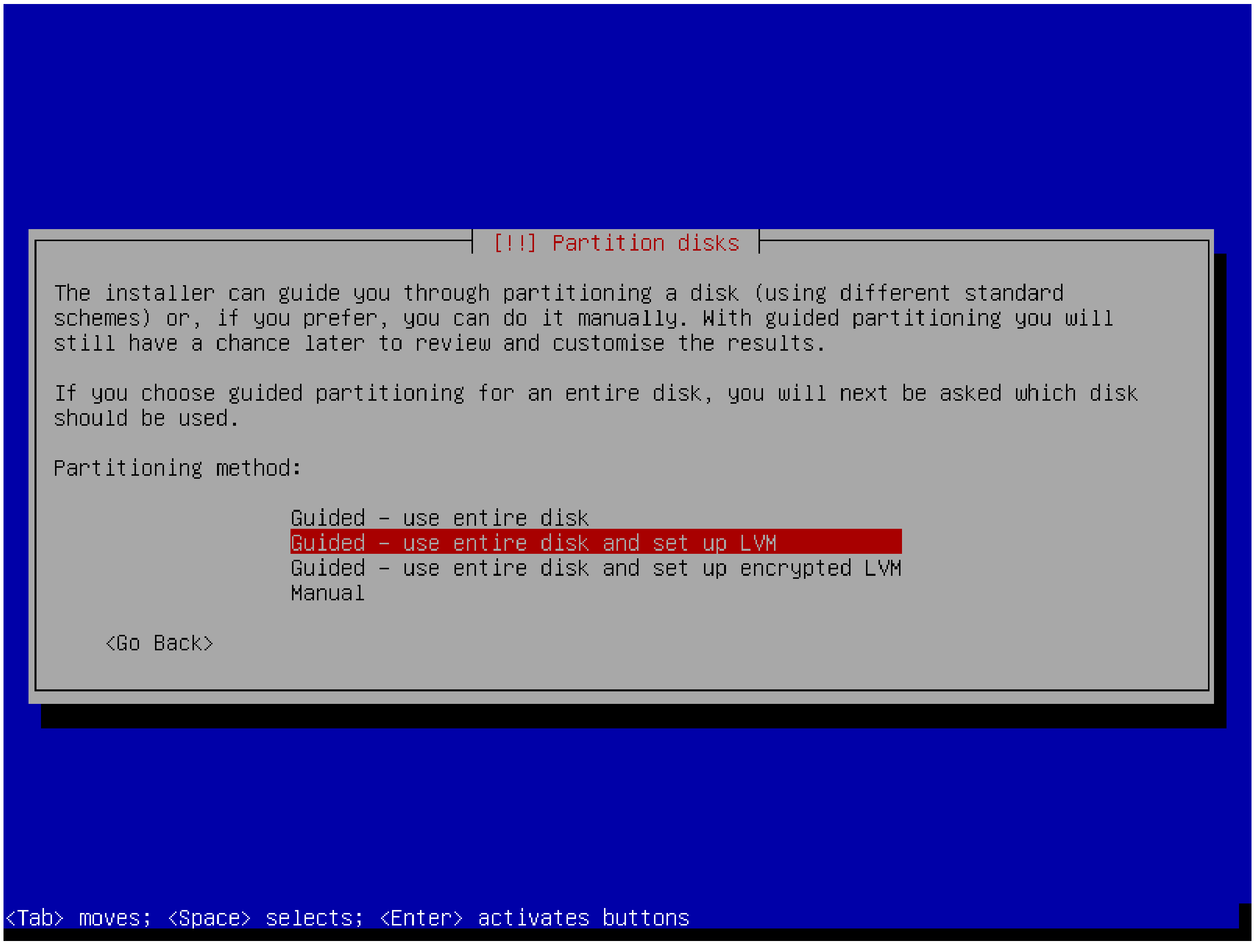
```
[!!] Set up users and passwords

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

toor

[*] Show Password in Clear

<Go Back>                                                    <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Re-enter your password, tab to Continue, and hit Enter.



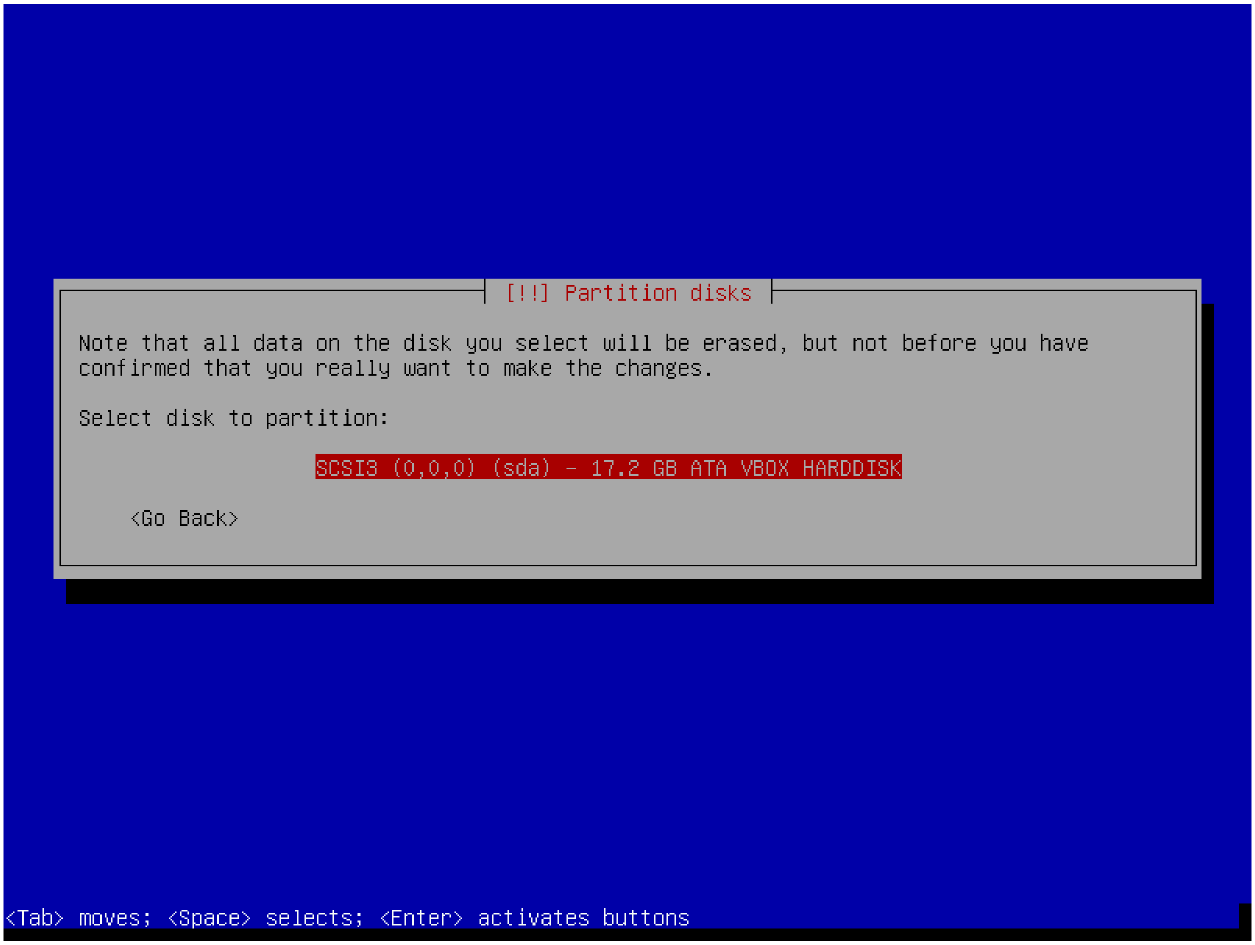
```
[!] Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language"
and select a country that uses the desired time zone (the country where you live or are
located).

Select your time zone:

                                      Eastern
                                      Central
                                      Mountain
                                      Pacific
                                      Alaska
                                      Hawaii
                                      Arizona
                                      East Indiana
                                      Samoa

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Select your timezone. Hit Enter.



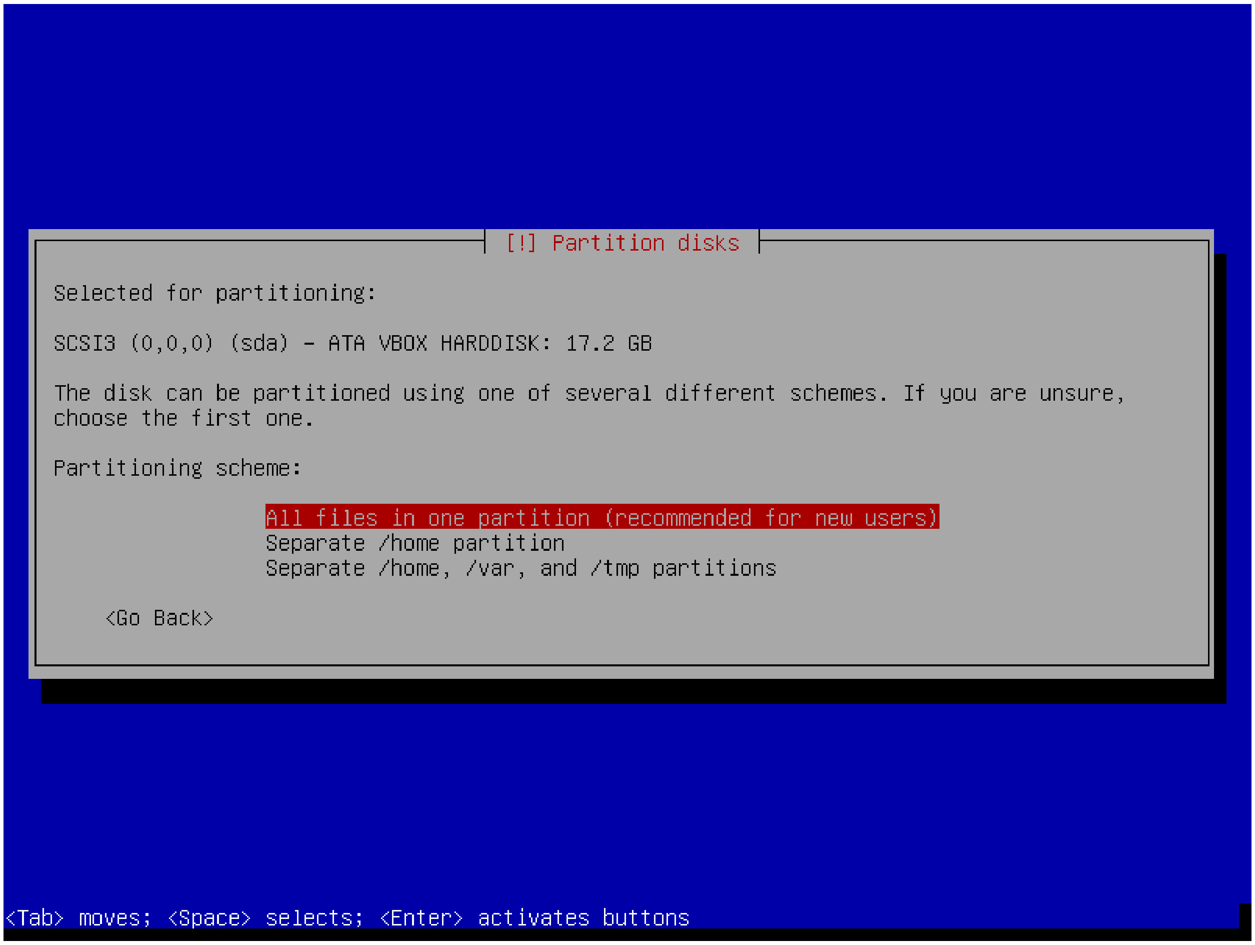
```
[!!] Partition disks

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

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

I chose Guided with LVM ti make my life easier. Plus I like the idea of adding another virtual disk, and being able to add that space to the existing volume. Hit Enter.



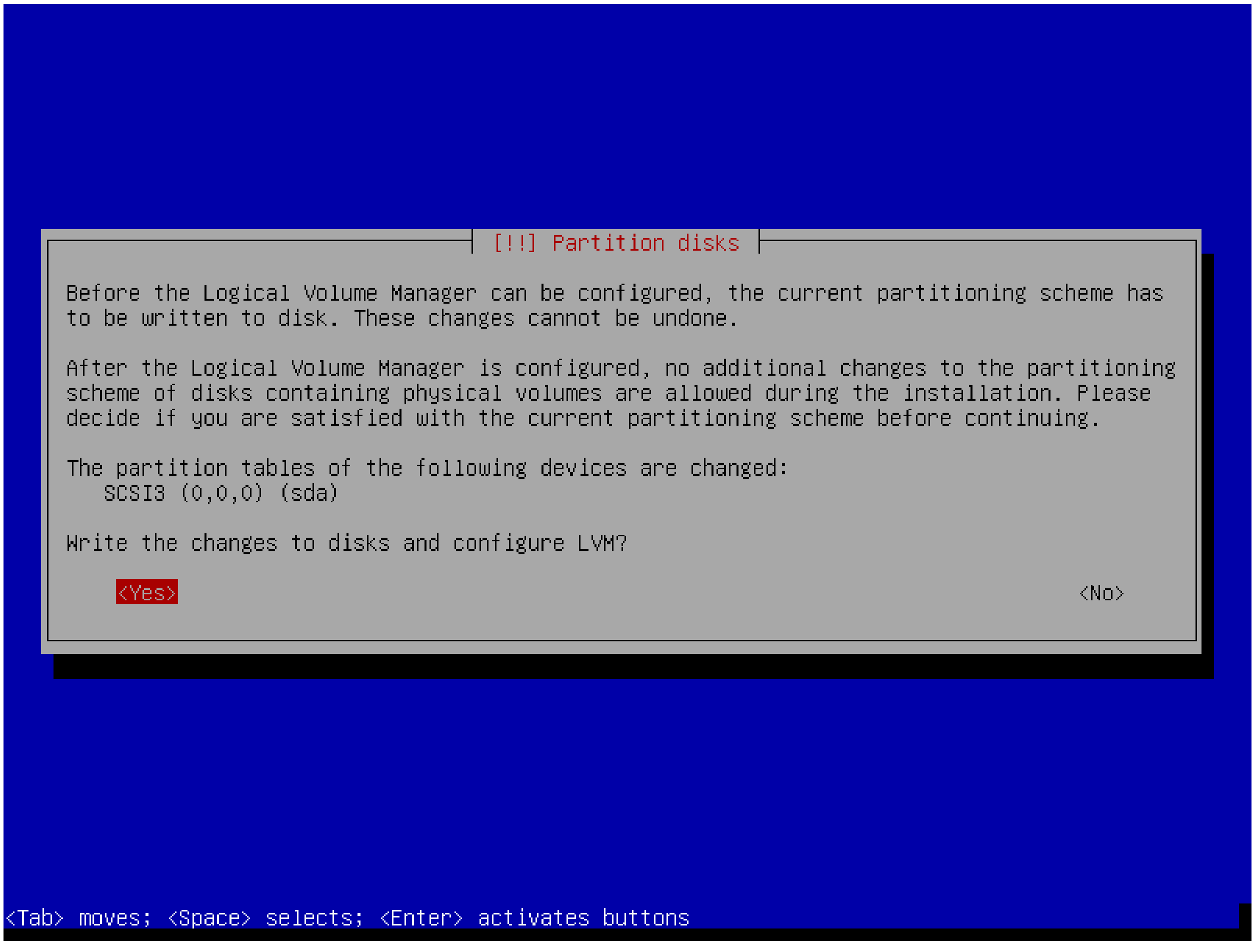
```
[!!] Partition disks

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:

                    SCSI3 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK

    <Go Back>
```

Select your disk and hit Enter.



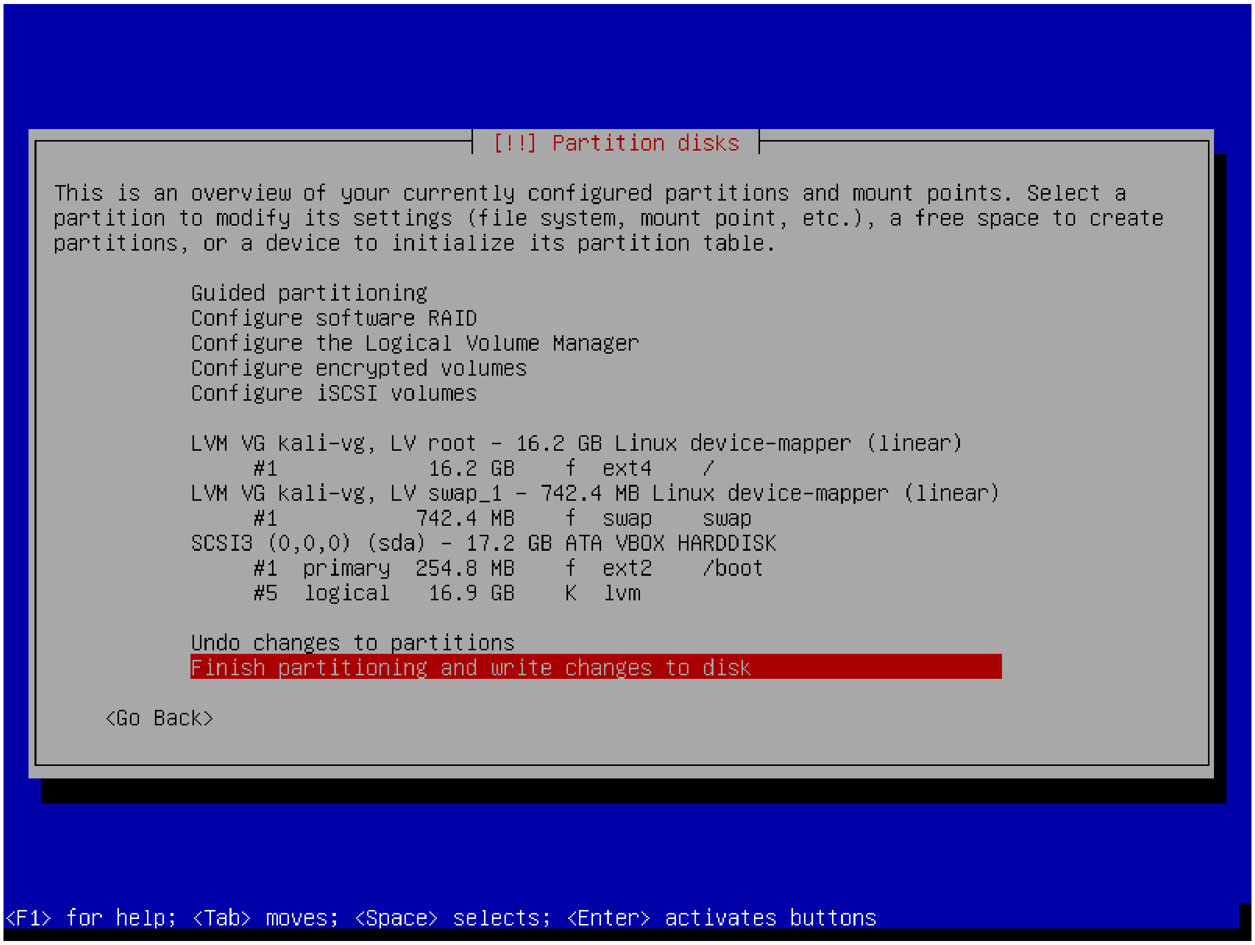
```
[!] Partition disks

Selected for partitioning:

SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 17.2 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

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Keep it simple and choose the first option. Hit Enter.



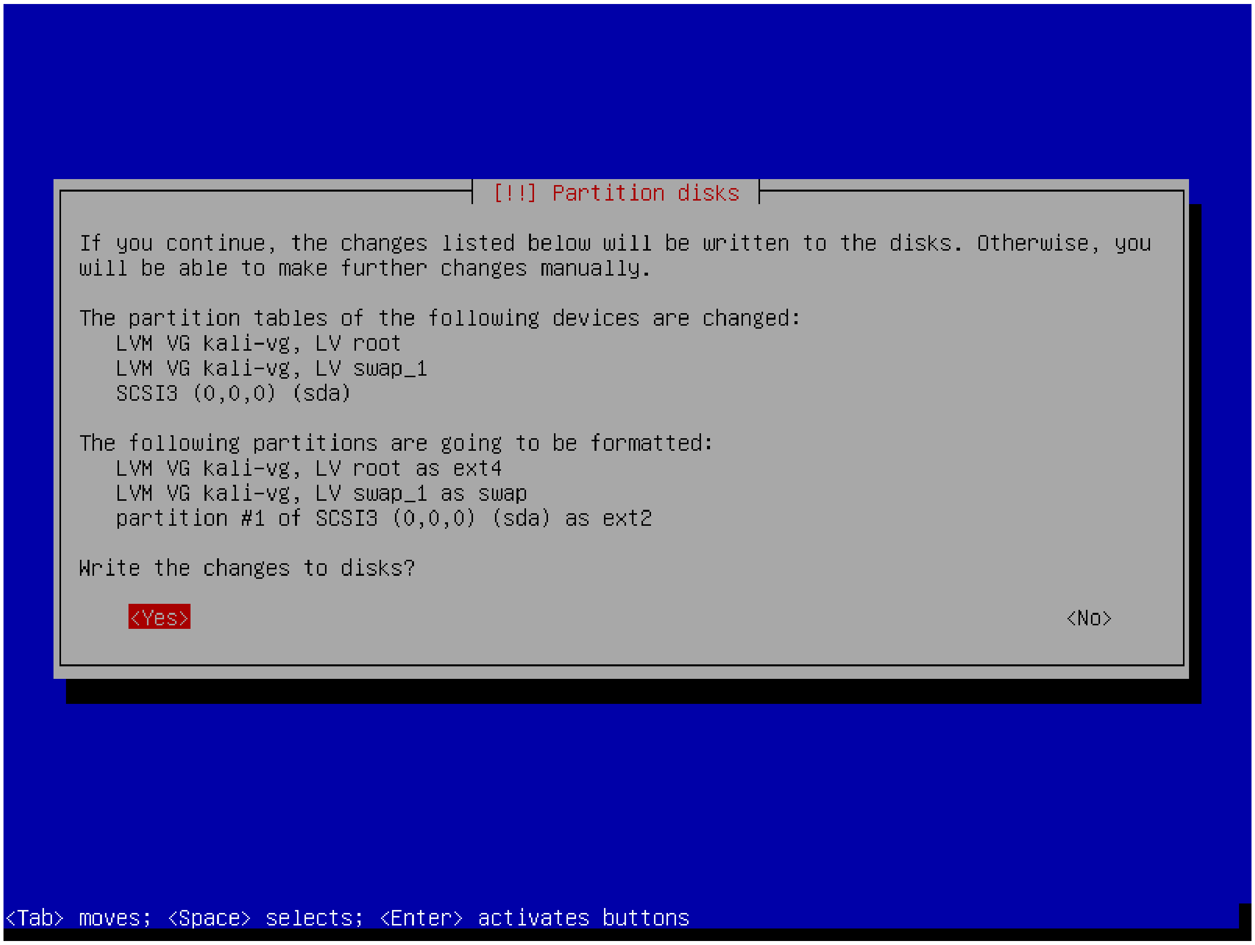
```
[!!] Partition disks

Before the Logical Volume Manager can be configured, the current partitioning scheme has
to be written to disk. These changes cannot be undone.

After the Logical Volume Manager is configured, no additional changes to the partitioning
scheme of disks containing physical volumes are allowed during the installation. Please
decide if you are satisfied with the current partitioning scheme before continuing.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

Write the changes to disks and configure LVM?

    <Yes>                                                                     <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Select Yes and hit Enter.



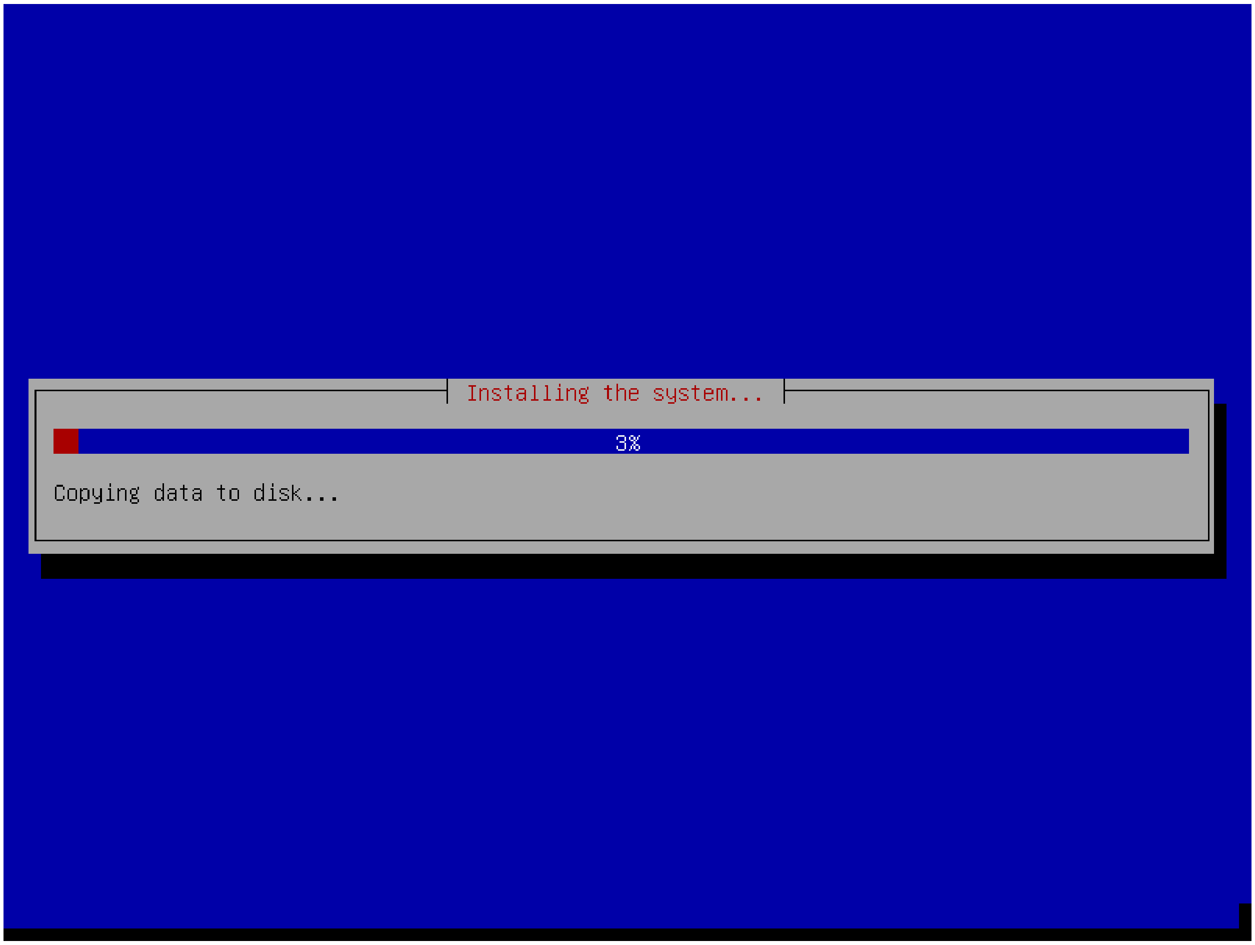
```
[!!] Partition disks

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

           LVM VG kali-vg, LV root - 16.2 GB Linux device-mapper (linear)
                #1            16.2 GB    f  ext4    /
           LVM VG kali-vg, LV swap_1 - 742.4 MB Linux device-mapper (linear)
                #1           742.4 MB    f  swap    swap
           SCSI3 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK
                #1  primary  254.8 MB    f  ext2    /boot
                #5  logical   16.9 GB    K  lvm

           Undo changes to partitions
           Finish partitioning and write changes to disk

    <Go Back>

<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons
```

Select the line with “Finish partitioning and write...” and hit Enter.



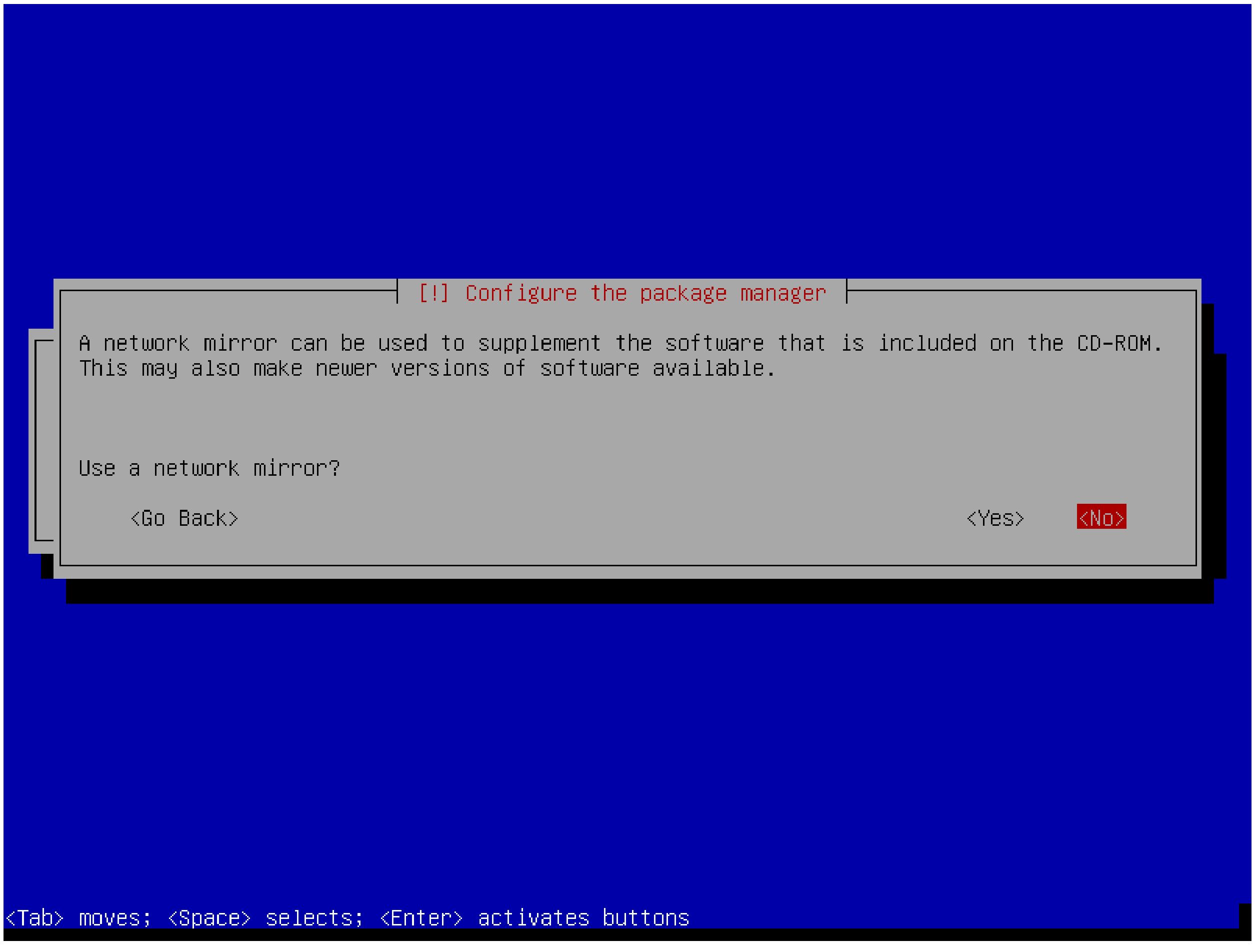
```
[!!] Partition disks

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:
   LVM VG kali-vg, LV root
   LVM VG kali-vg, LV swap_1
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   LVM VG kali-vg, LV root as ext4
   LVM VG kali-vg, LV swap_1 as swap
   partition #1 of SCSI3 (0,0,0) (sda) as ext2

Write the changes to disks?
```

Select Yes and hit Enter.



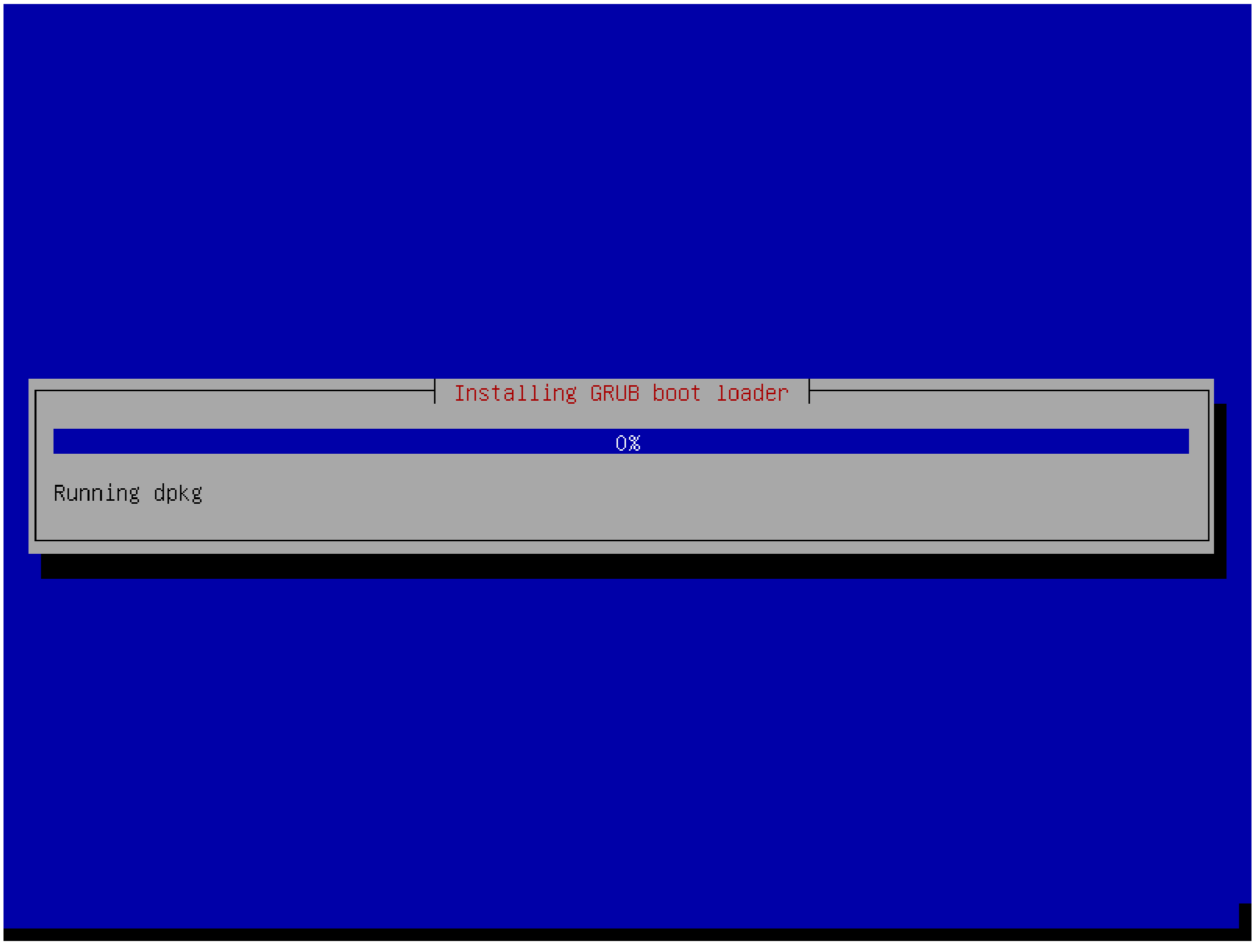
```
Installing the system...

3%

Copying data to disk...
```

The installation will begin.



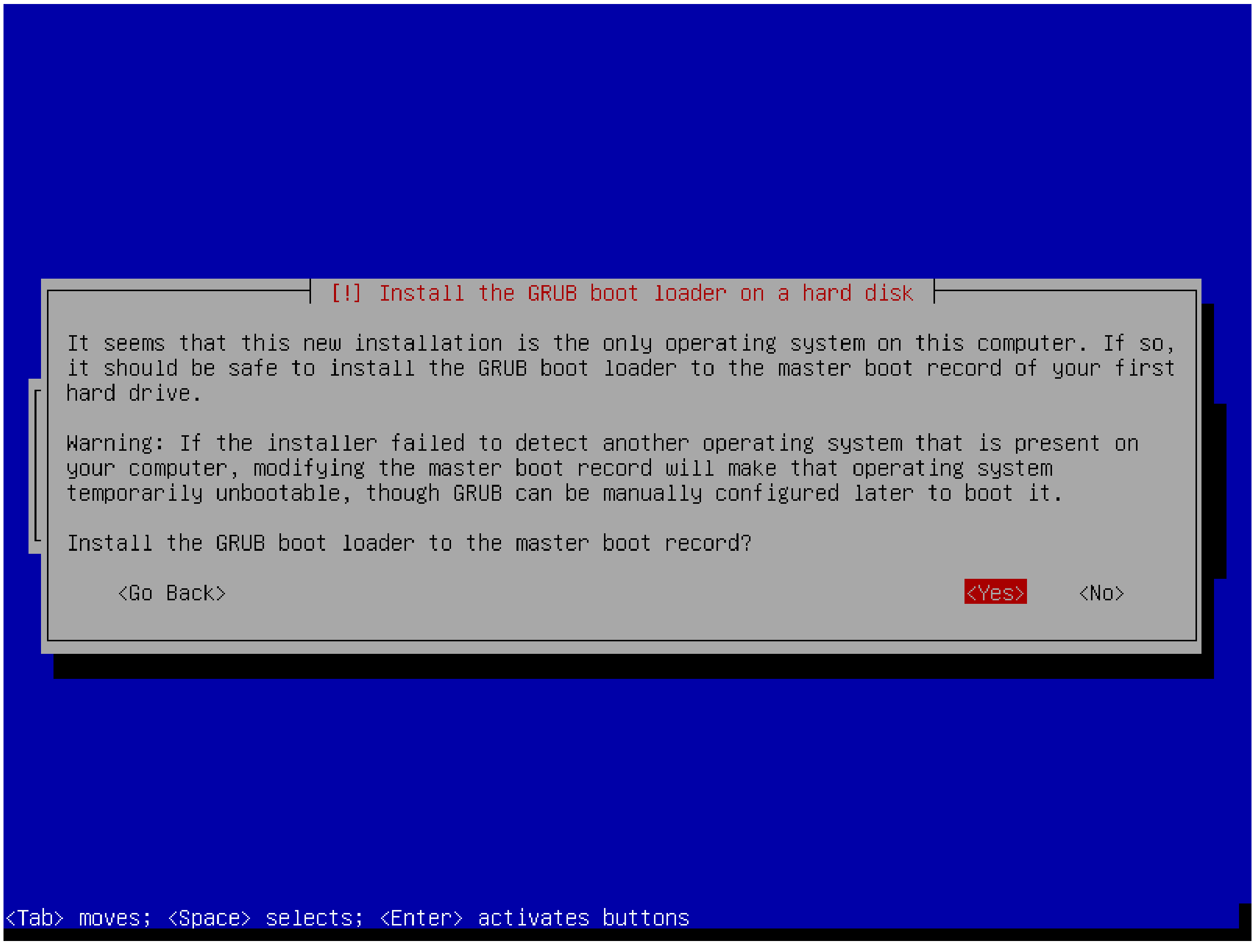
```
[!] Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM.
This may also make newer versions of software available.


Use a network mirror?
```

Since this is going to be an isolated system, there is no reason to spend the time setting up updates. Select No and hit Enter.



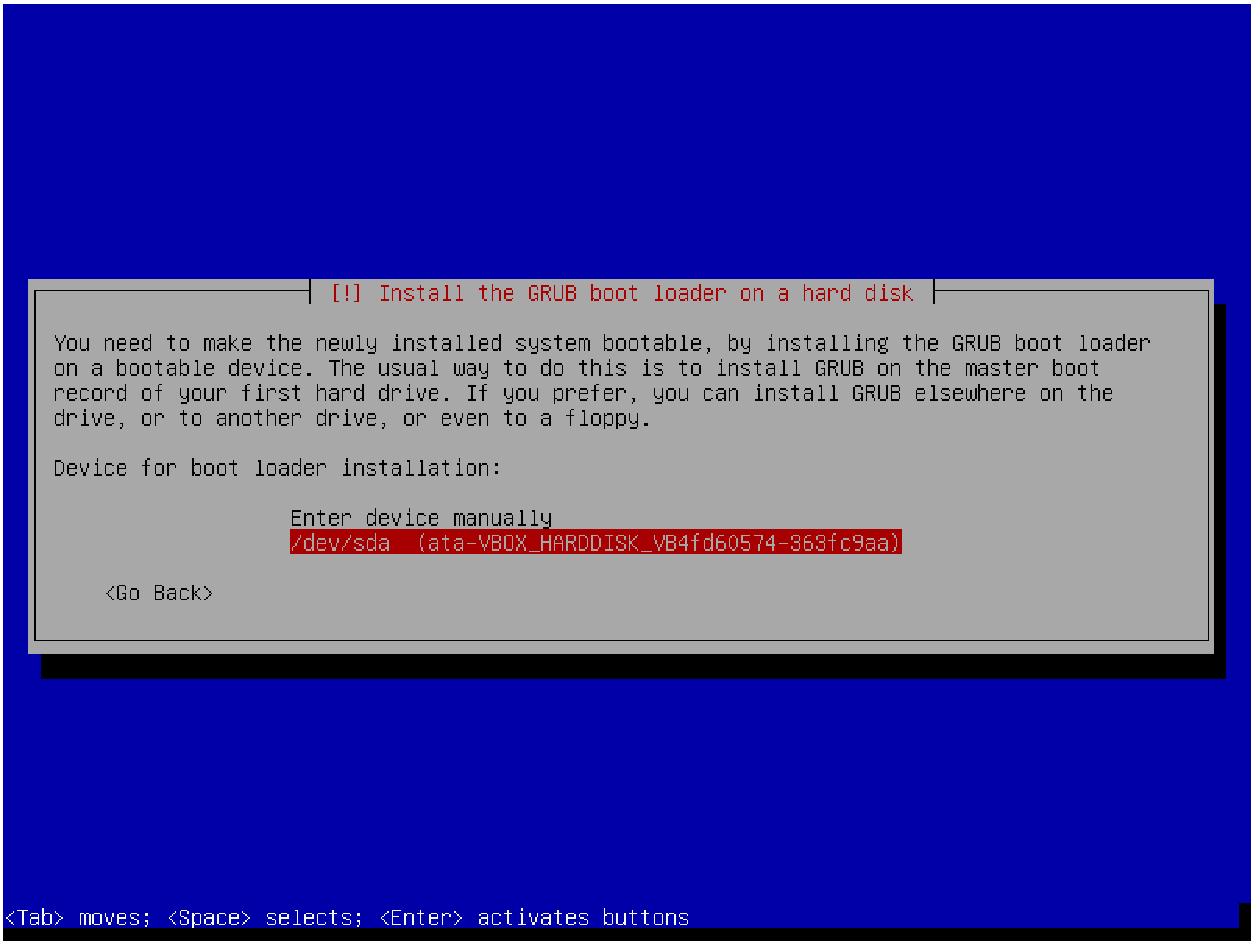
```
Installing GRUB boot loader

0%

Running dpkg
```

The system will finish installing and finally configure the GRUB boot loader.



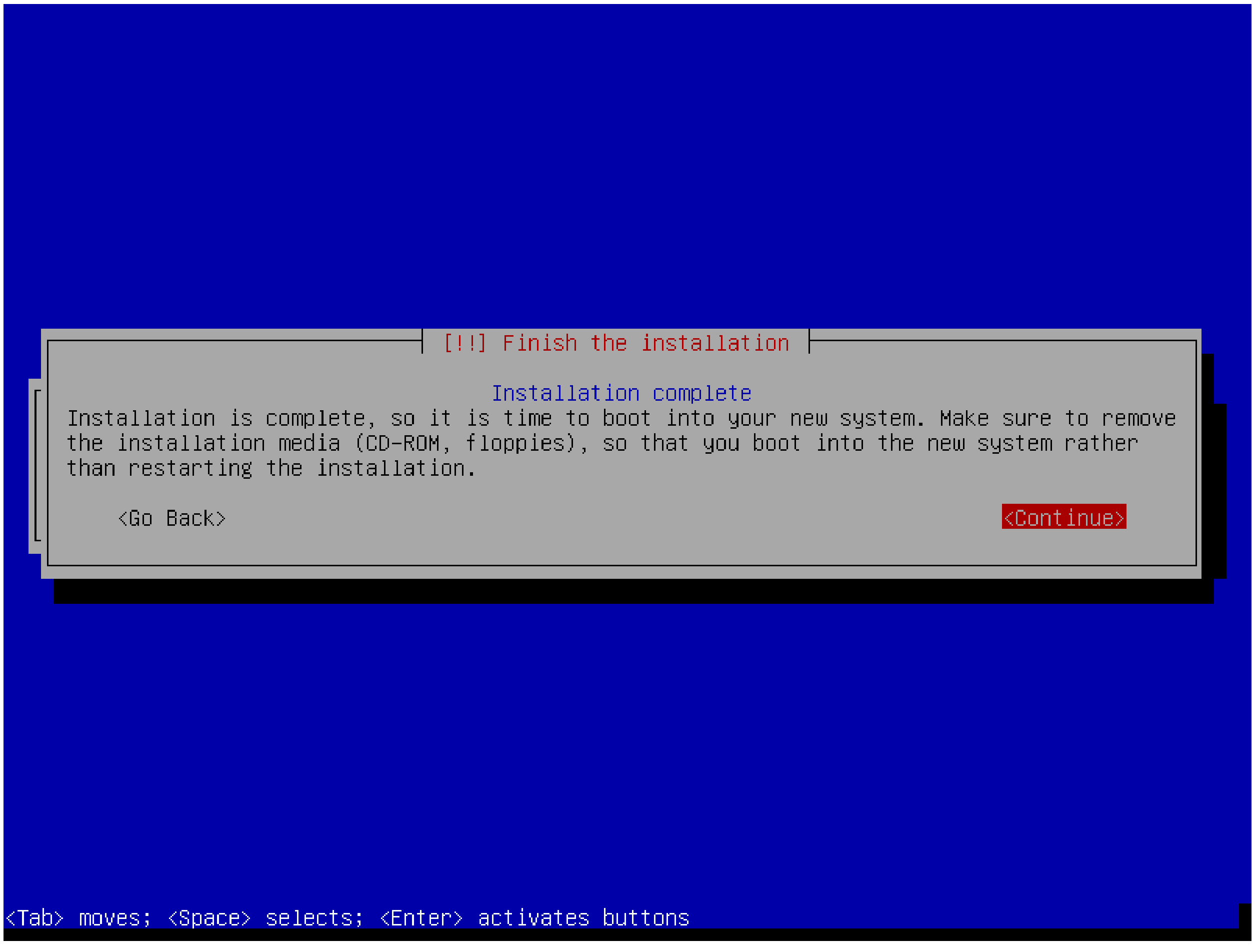
```
[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so,
it should be safe to install the GRUB boot loader to the master boot record of your first
hard drive.

Warning: If the installer failed to detect another operating system that is present on
your computer, modifying the master boot record will make that operating system
temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

    <Go Back>                                                          <Yes>    <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Select Yes and hit Enter.



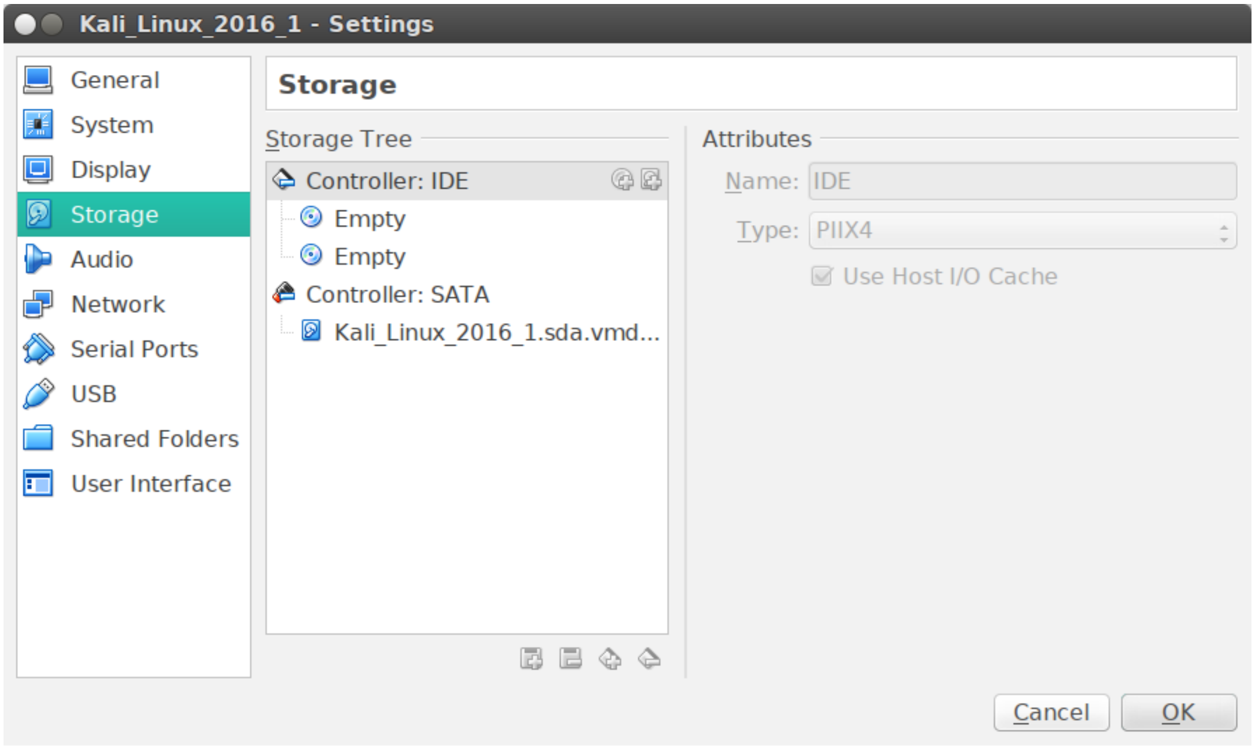
```
[!] Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader
on a bootable device. The usual way to do this is to install GRUB on the master boot
record of your first hard drive. If you prefer, you can install GRUB elsewhere on the
drive, or to another drive, or even to a floppy.

Device for boot loader installation:

                    Enter device manually
                    /dev/sda  (ata-VBOX_HARDDISK_VB4fd60574-363fc9aa)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Select your hard drive and hit Enter.



```
[!!] Finish the installation

Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove
the installation media (CD-ROM, floppies), so that you boot into the new system rather
than restarting the installation.
```

Select Continue and hit Enter. On my VirtualBox system, the install media already disconnected the ISO image, so I don’t have to stop the system and disconnect the image before rebooting (otherwise you would boot back to the Live CD).



Kali_Linux_2016_1 - Settings

Storage

Storage Tree

- Controller: IDE
  - Empty
  - Empty
- Controller: SATA
  - Kali_Linux_2016_1.sda.vmd...

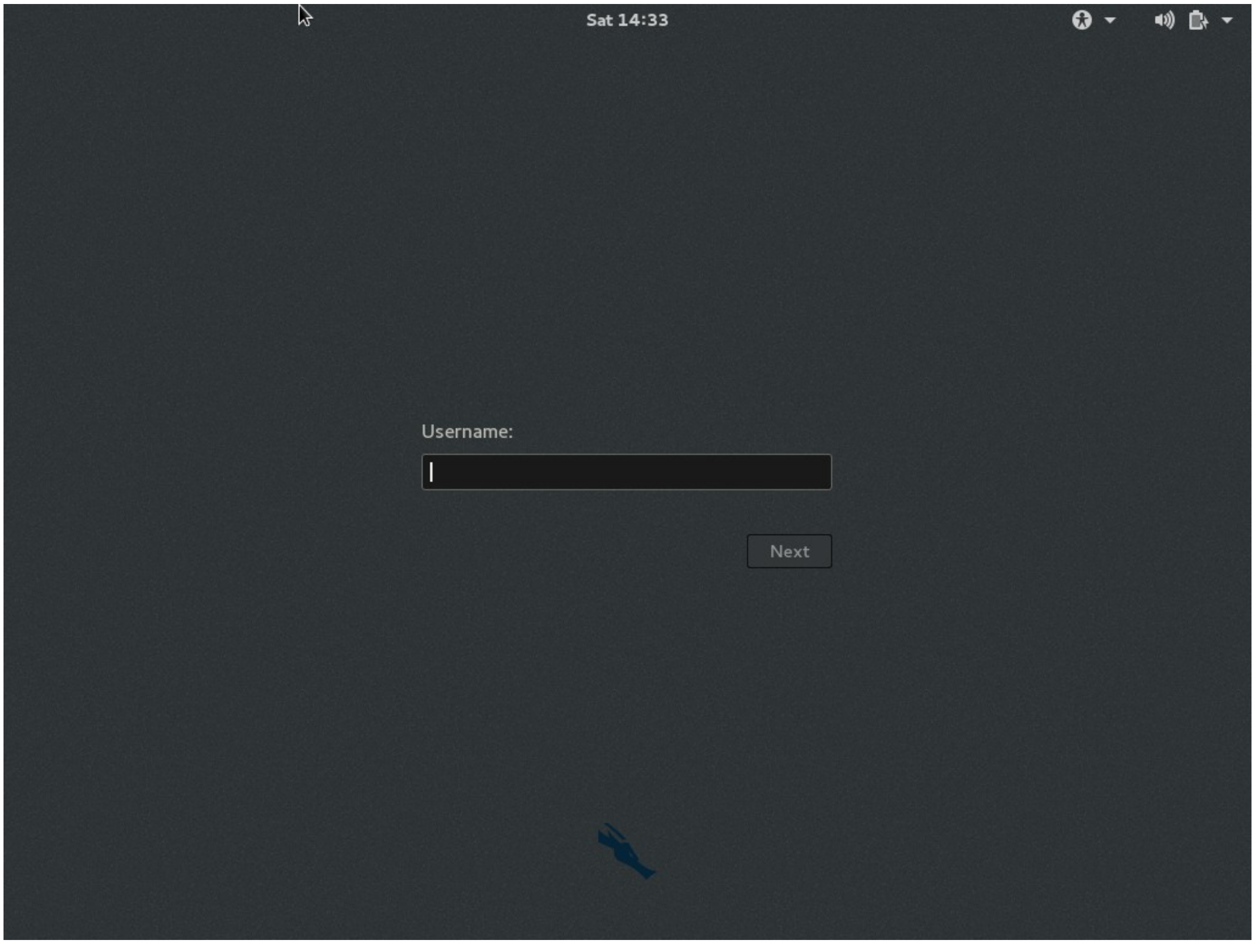
Attributes

Name: IDE

Type: PIIX4

☑ Use Host I/O Cache

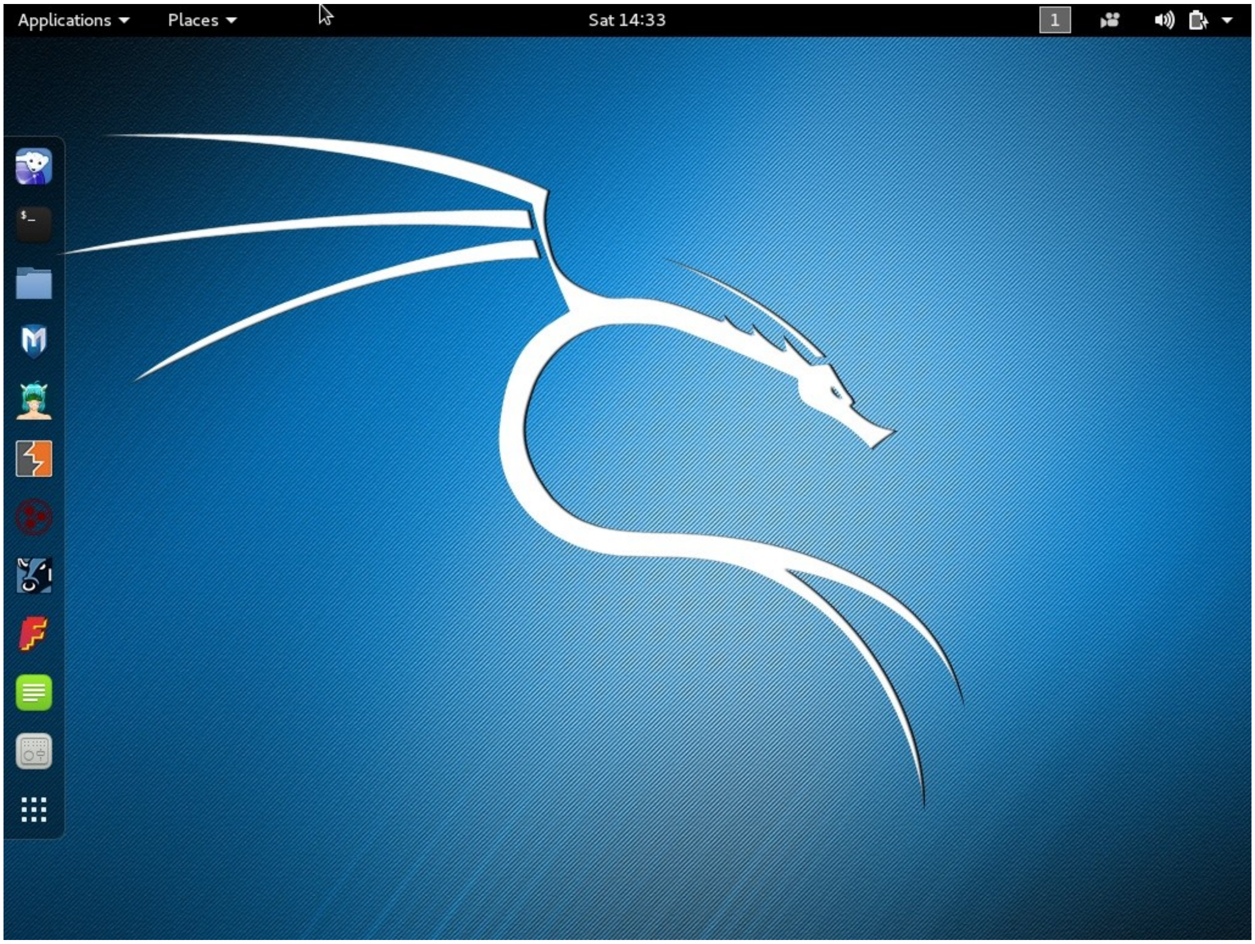
This is what your settings should look like. Again, it seems like the installer is able to unmount the ISO from virtualbox.



Sat 14:33

Username:

On boot, this is what you should see. Login as root with your root password.



Initial login screen. From here, some friendly tool, like a Terminal on the left panel to get started.

This concludes the install of Kali Linux.

Conclusion

By following the above steps, you will have a working instance of Kali Linux. I prefer this over running a Live CD because I can save data and results (you could do the same from a Live CD with a thumb drive plugged in). I'm not doing anything nefarious here, the point of this is for having a repeatable environment to tinker with and save the results for further research. Future papers will then use this instance as the backbone for attacking the DVL instance. Make sure both instances have their network adapters configured to use the Host-only interface. I cannot stress this enough.

Post Review/Action

I discovered after installing that I wanted to have 2 network interfaces. I adjusted the virtual machine for two, one attached to 192.168.139-NAT and the second attached to Host-only with vboxnet0. I plan on updating Kali Linux when I need to, but before I scan a target, I will disable the first network interface, 192.168.139-NAT. This way, the scans are truly isolated. I don’t want any network traffic, DNS or anything leaving my laptop when performing vulnerability assessments. OWASP ZAP can run isolated, but firing up the engine and performing an update every once in a while is not a bad idea. Just make sure to disable the NAT’ed interface before scanning. You’ve been warned!