--> -->

January 21, 2019 *by Michael Bose*

How to Install Kali Linux on VMware VM

Kali is a free Debian-based Linux distribution intended for penetration testing. The first version of Kali Linux was released in 2013 as the rebuild of BackTrack Linux – a previous well-known distribution for security auditing and penetration testing. Some tools that were duplicated or provided similar functionality in BackTrack Linux were removed in Kali Linux. There are more than 600 penetration testing tools included in Kali Linux that can be run as Live DVD without installation as well as be installed on a computer as a desktop OS.

Sometimes you may not have the ability to dedicate the entire computer to running Kali Linux from neither Live DVD nor your internal hard disk as the installed OS. In this case, hardware virtualization technologies can help you – you can install Kali Linux on a VMware VM running on your desktop, laptop, or server. As a result, you can use your physical machine for the usual tasks while simultaneously running a virtual machine with Kali Linux for penetration testing and security auditing of your networks, software, etc. This blog post explores the installation process of Kali Linux on a VMware virtual machine and configuration of a Wi-Fi network adapter.

Downloading the ISO Image

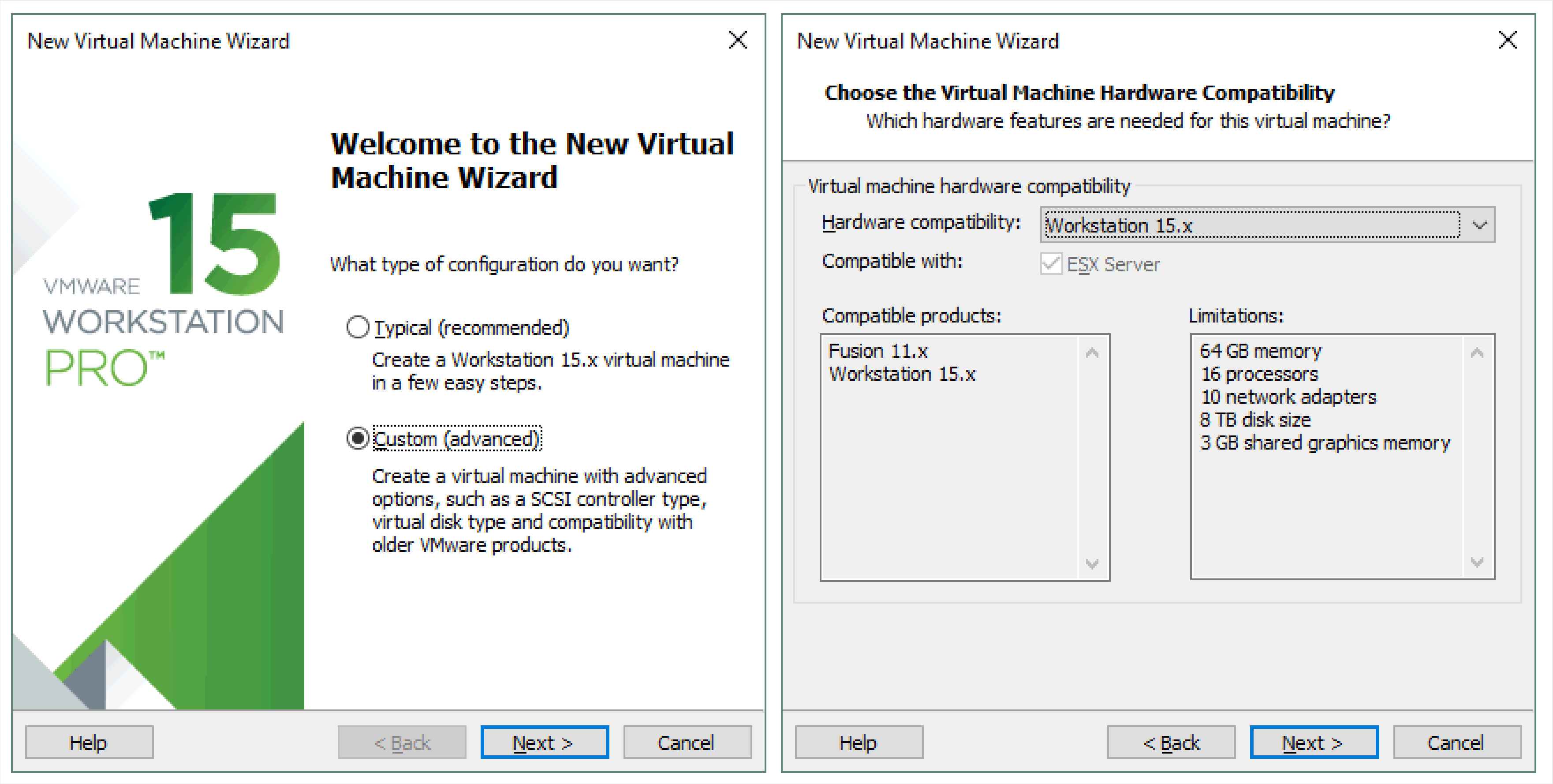
First, open the Kali download page in your browser and select the distribution that can best meet your needs. The installation images are provided in the ISO format for 32bit, 64bit and ARM architecture. You can also select the build with your favorite graphics desktop environment among Gnome, KDE, Xfce, Mate, etc. For the sake of simplicity and consistency in this blog post, let's download *Kali Linux Xfce 64 Bit* via HTTP. When the ISO file is downloaded, check the **sha256sum to verify the data integrity and ensure that the file is not corrupted.**

Creating a New VMware VM

Let's explore how to install Kali Linux on a VM of the VMware Workstation format due to portability-related reasons – you can install VMware Workstation on a laptop, deploy a virtual machine with Kali Linux, and use this laptop for auditing wireless networks, for example. Kali Linux can also be installed on a VMware ESXi host if needed – the installation process is quite similar. In the current example, VMware Workstation 15 will be used to show the installation and configuration of Kali Linux.

Click **File > New virtual machine** to open the New Virtual Machine Wizard. Select **Custom**.

Choose the virtual machine hardware compatibility. If you are not planning to migrate a VM to older versions of VMware Workstation or ESXi servers, select the Workstation 15.x format. In this example the Workstation 14.x format should be selected for better compatibility in case of possible migration.



Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

○ Typical (recommended)

Create a Workstation 15.x virtual machine in a few easy steps.

● Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Choose the Virtual Machine Hardware Compatibility

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 15.x

Compatible with: ☑ ESX Server

Compatible products:

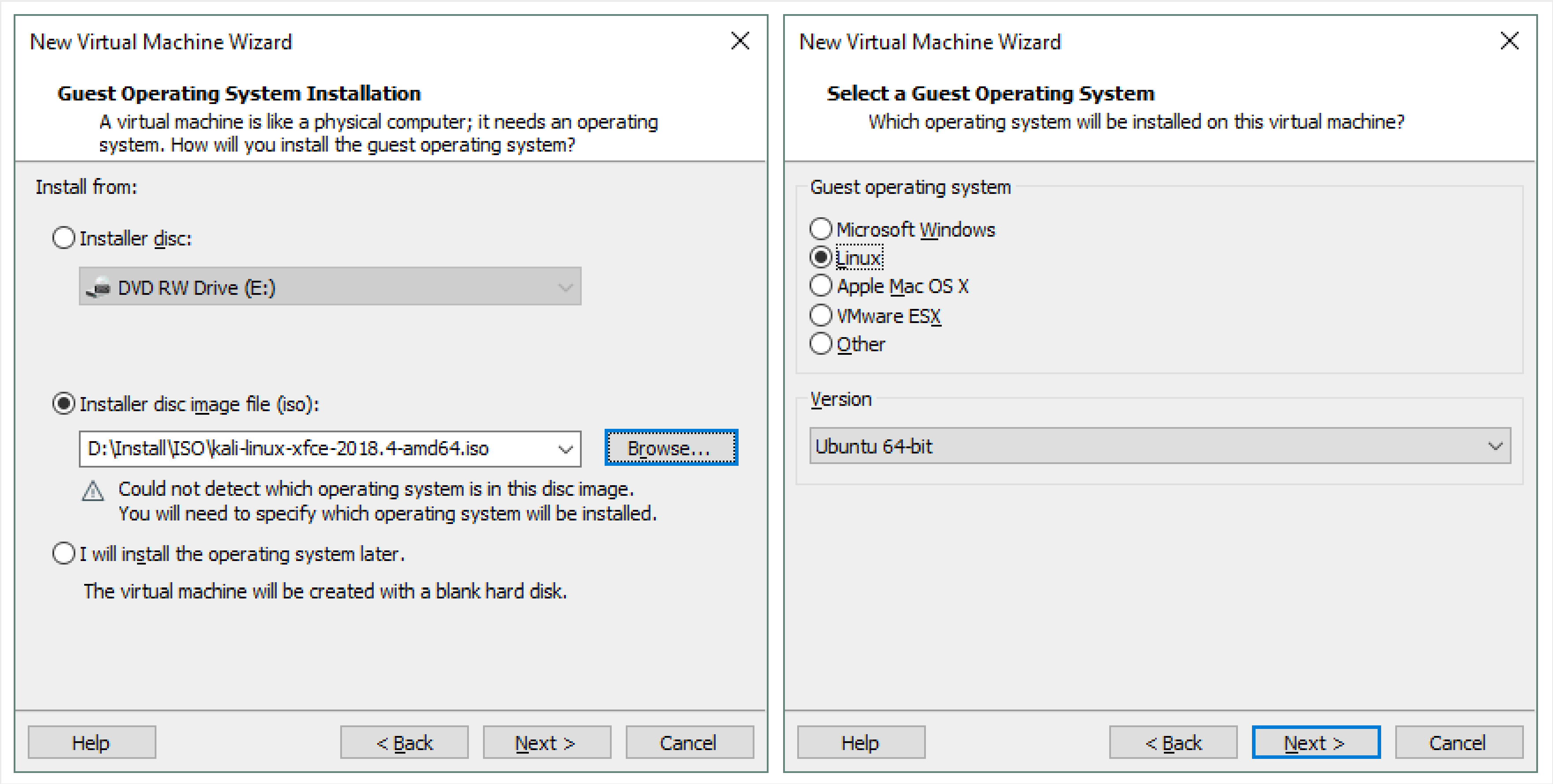
Fusion 11.x
Workstation 15.x

Limitations:

64 GB memory
16 processors
10 network adapters
8 TB disk size
3 GB shared graphics memory

Select the installer disk image file for guest operating system installation. In this case the downloaded ISO image saved to *D:\Install\ISO\kali-linux-xfce-2018.4-amd64.iso* should be selected.

Select a guest operating system (OS). Linux Ubuntu 64-bit must be selected for our purposes.



New Virtual Machine Wizard

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (E:)

● Installer disc image file (iso):

D:\Install\ISO\kali-linux-xfce-2018.4-amd64.iso

Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

New Virtual Machine Wizard

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system

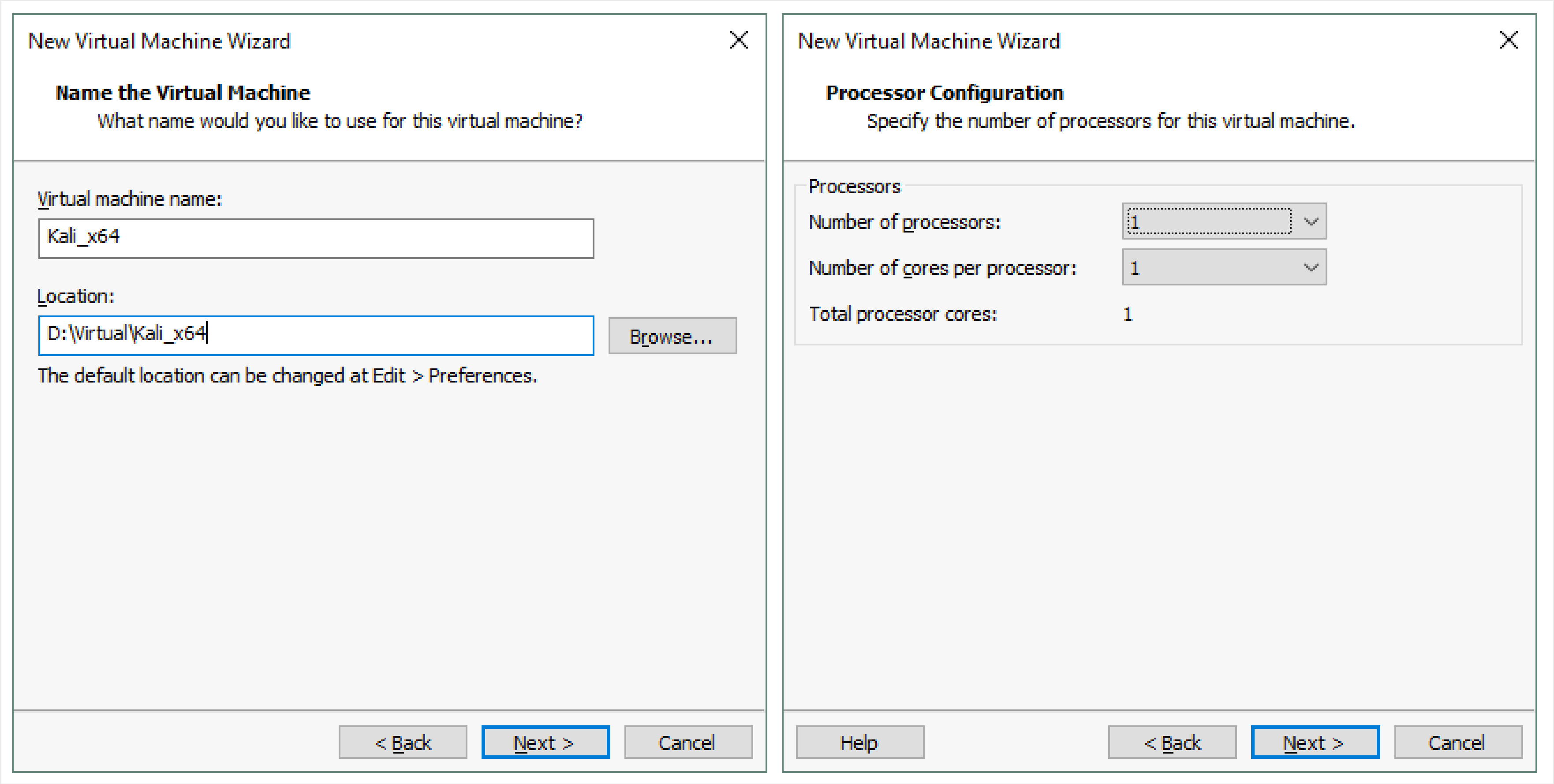
○ Microsoft Windows
● Linux
○ Apple Mac OS X
○ VMware ESX
○ Other

Version

Ubuntu 64-bit

Specify the VM name and location. In the current example, the VM name is Kali_x64 and the VM directory is D:\Virtual\Kali_x64.

Processor configuration. Specify the number of processors and the number of cores per processor for this virtual machine. Using 1 CPU is enough for Kali Linux.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Kali_x64

Location: D:\Virtual\Kali_x64

The default location can be changed at Edit > Preferences.

New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

Processors

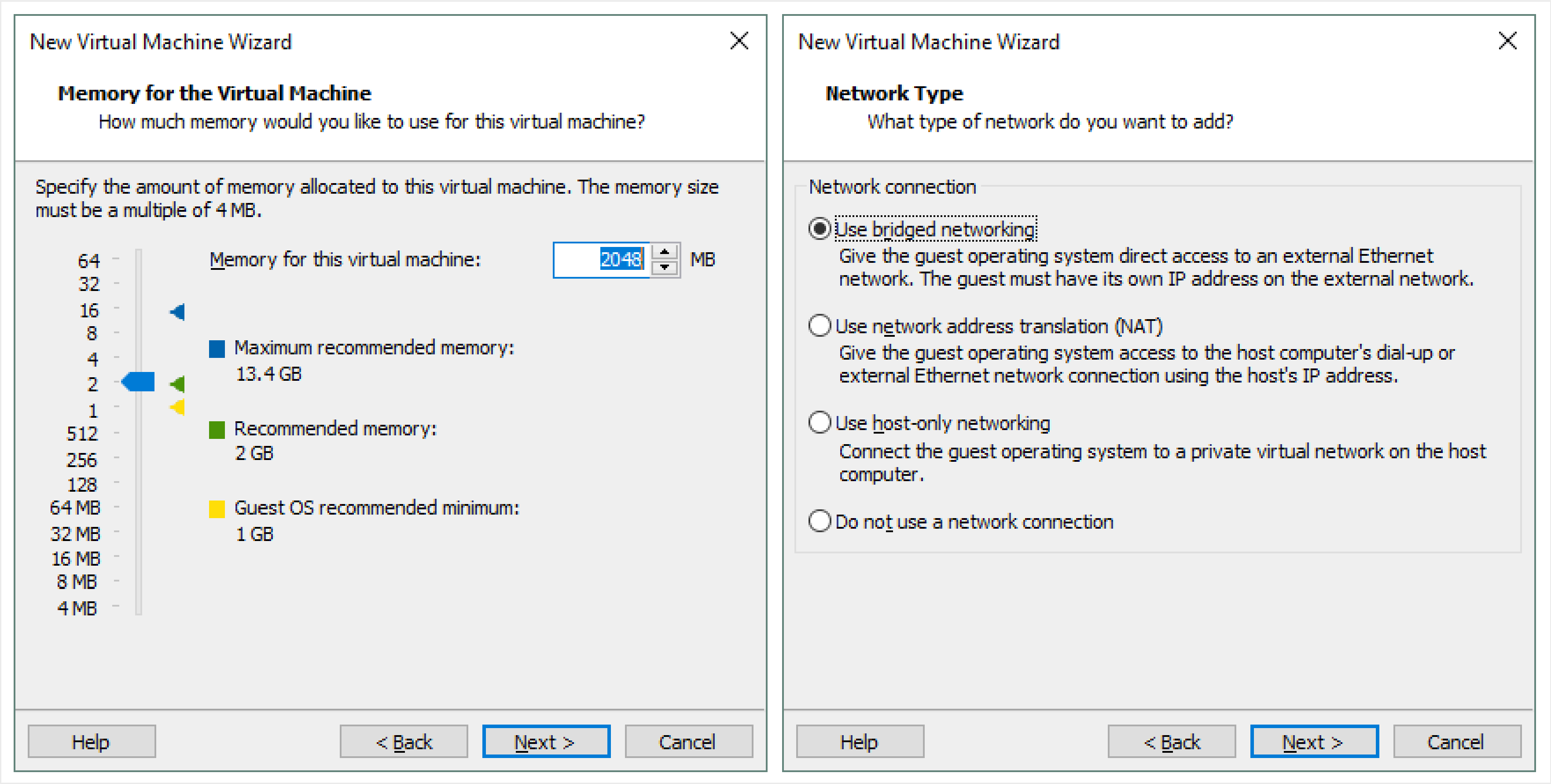
Number of processors: 1

Number of cores per processor: 1

Total processor cores: 1

Set memory for the virtual machine. Kali Linux is not a resource-hungry operating system. 2 GB of memory should be more than enough for this VM.

Configure a network type for the VM. Select the **Use bridged networking** option.



New Virtual Machine Wizard

Memory for the Virtual Machine
How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

🟦 Maximum recommended memory:
13.4 GB

🟩 Recommended memory:
2 GB

🟨 Guest OS recommended minimum:
1 GB

New Virtual Machine Wizard

Network Type
What type of network do you want to add?

Network connection

● Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

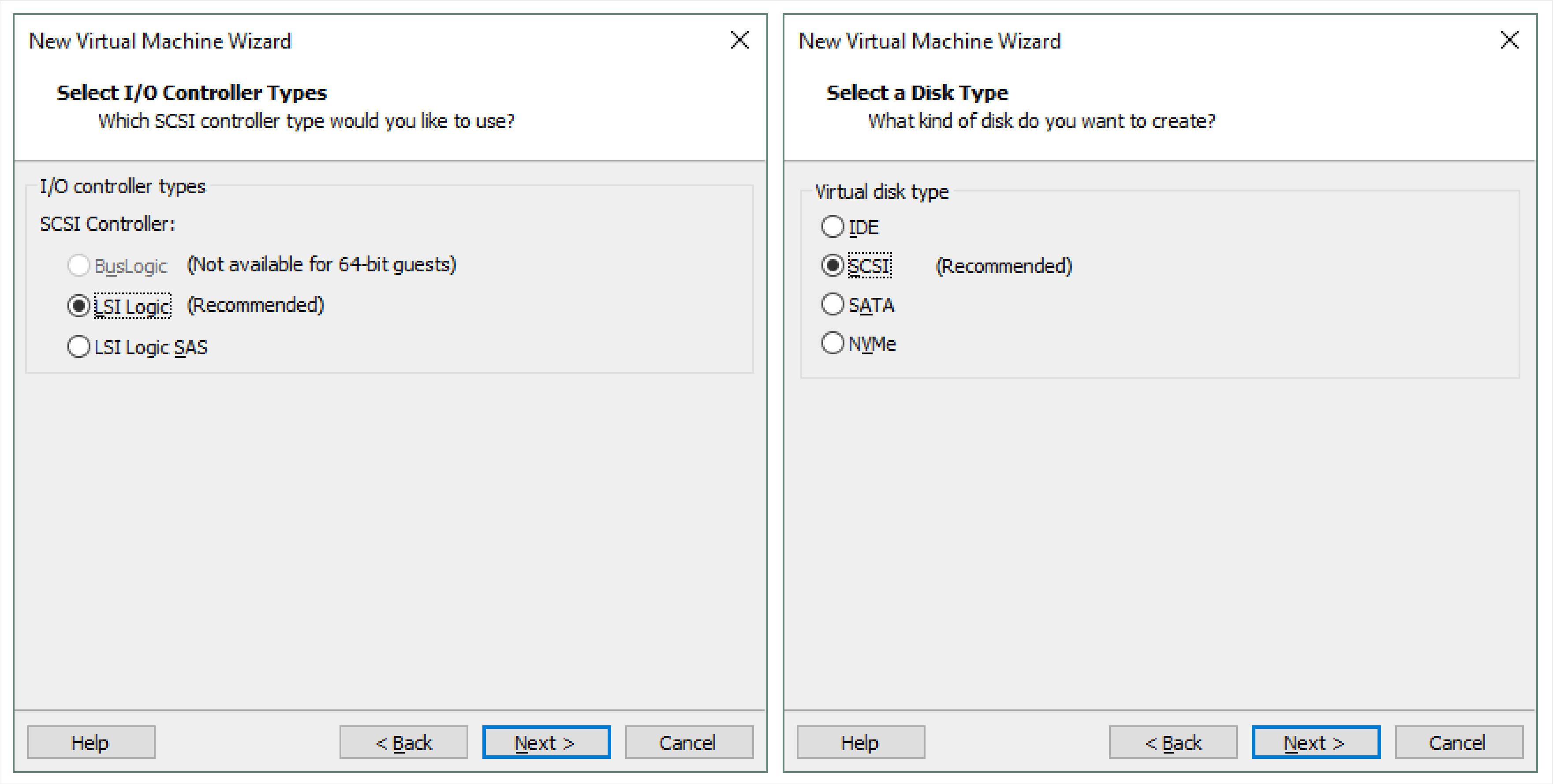
○ Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

Select the SCSI controller that you will use for connecting a virtual disk to a VM. You can leave the default value as is and click **Next** to continue.

Select a disk type. You can leave the default recommended value (SCSI).


New Virtual Machine Wizard

Select I/O Controller Types

Which SCSI controller type would you like to use?

I/O controller types

SCSI Controller:

○ BusLogic (Not available for 64-bit guests)

● LSI Logic (Recommended)

○ LSI Logic SAS

New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

○ IDE

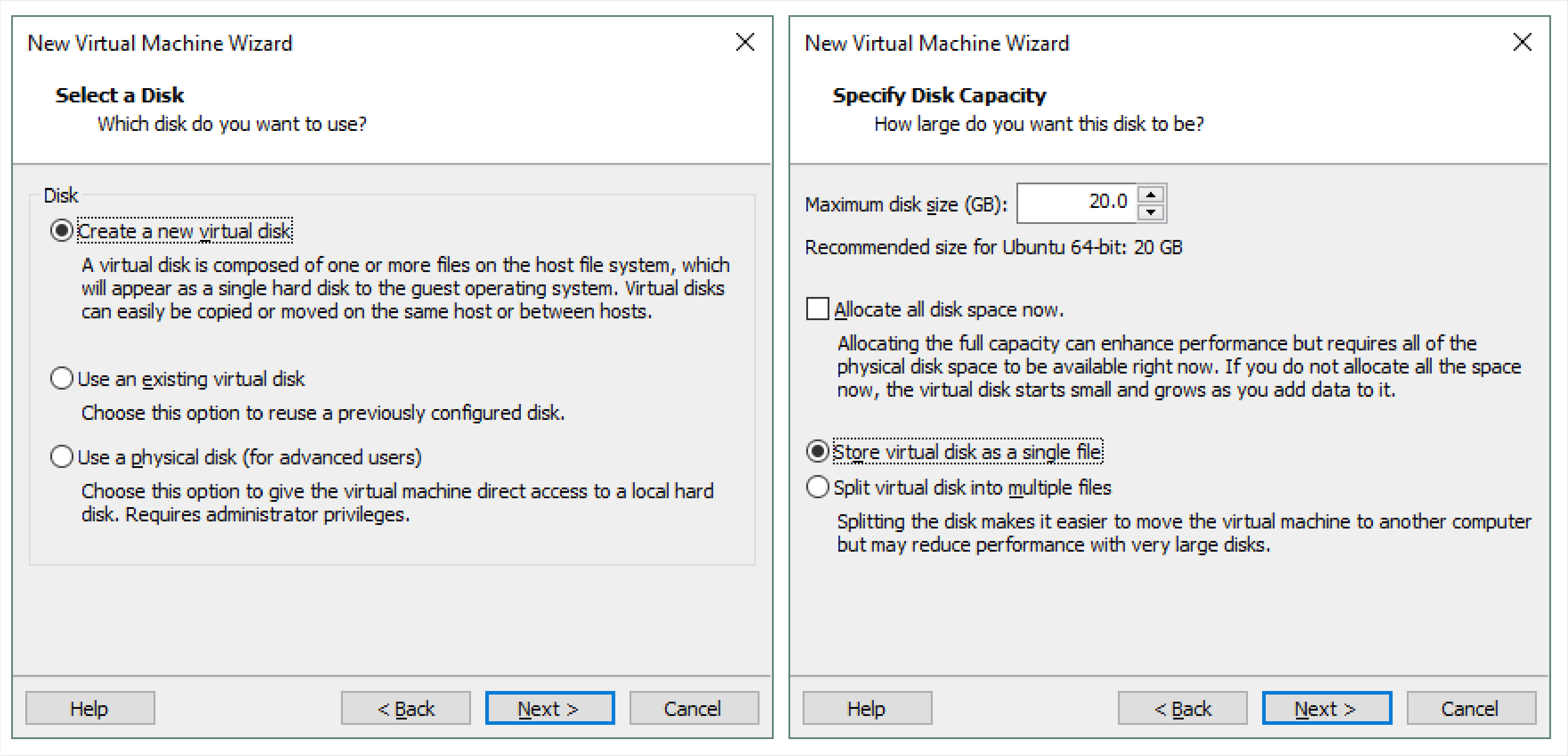
● SCSI (Recommended)

○ SATA

○ NVMe

Select a disk. Click **Create a new virtual disk** and then click **Next.**

Specify disk capacity. 20 GB should be enough for the operating system. Select **Store virtual disk as a single file** if there are no limitations of your file system (such as 4 GB limit of file size for FAT32). Don't check the box **Allocate all disk space now** if you don't want the disk to consume all provisioned disk space now.



New Virtual Machine Wizard

Select a Disk
Which disk do you want to use?

Disk

● Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

○ Use an existing virtual disk

Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

Maximum disk size (GB): 20.0

Recommended size for Ubuntu 64-bit: 20 GB

□ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

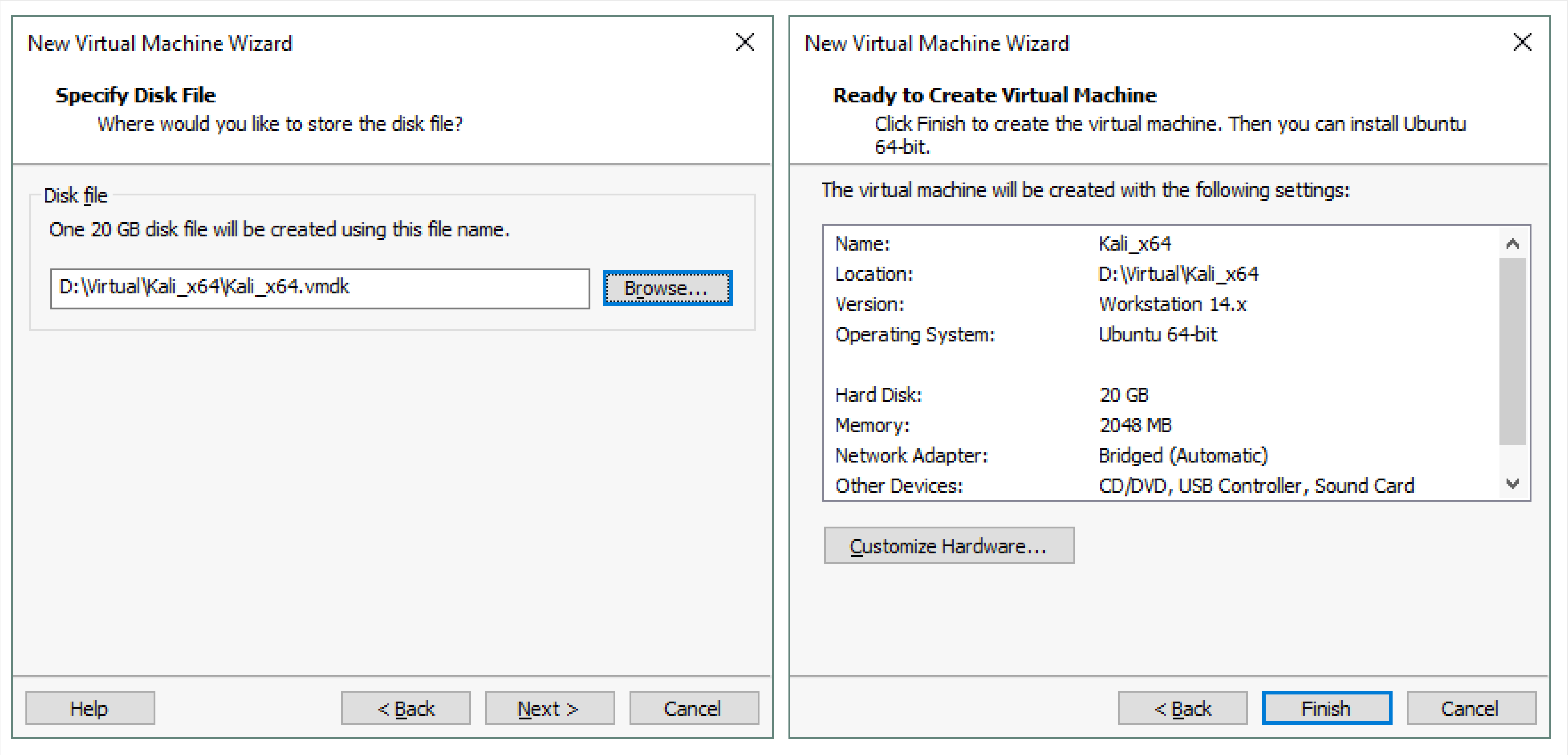
● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Specify where you want to store the virtual disk file. In this example, the file path is D:\Virtual\Kali_x64\Kali_x64.vmdk.

Now everything is ready to create a virtual machine. Check the VM settings, customize hardware if necessary, and click **Finish** to create a VM.



New Virtual Machine Wizard

Specify Disk File
Where would you like to store the disk file?

Disk file
One 20 GB disk file will be created using this file name.

D:\Virtual\Kali_x64\Kali_x64.vmdk

New Virtual Machine Wizard

Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Ubuntu 64-bit.

The virtual machine will be created with the following settings:

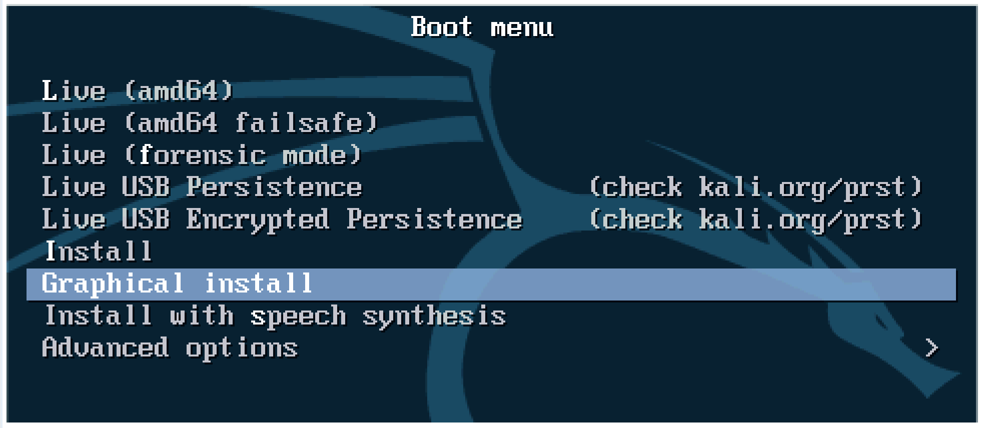
Name:	Kali_x64
Location:	D:\Virtual\Kali_x64
Version:	Workstation 14.x
Operating System:	Ubuntu 64-bit
Hard Disk:	20 GB
Memory:	2048 MB
Network Adapter:	Bridged (Automatic)
Other Devices:	CD/DVD, USB Controller, Sound Card

Deploying Kali Linux on VMware VM

Installing Kali Linux is not difficult, as all installation steps are supplied with useful tips and comments. Let’s review the installation process step by step:

Installing the Operating System

Once you have created a new VM, power on that VM and boot from the ISO image to start Kali installation. When a VM is loaded from the ISO image, you can see a boot menu that allows you to boot from the installation media in a live DVD mode, install the OS in a text mode (you get only a console interface without graphical user interface (GUI) after installation), and install the OS in graphical mode. Select **Graphical install** from the boot menu and press **Enter**.

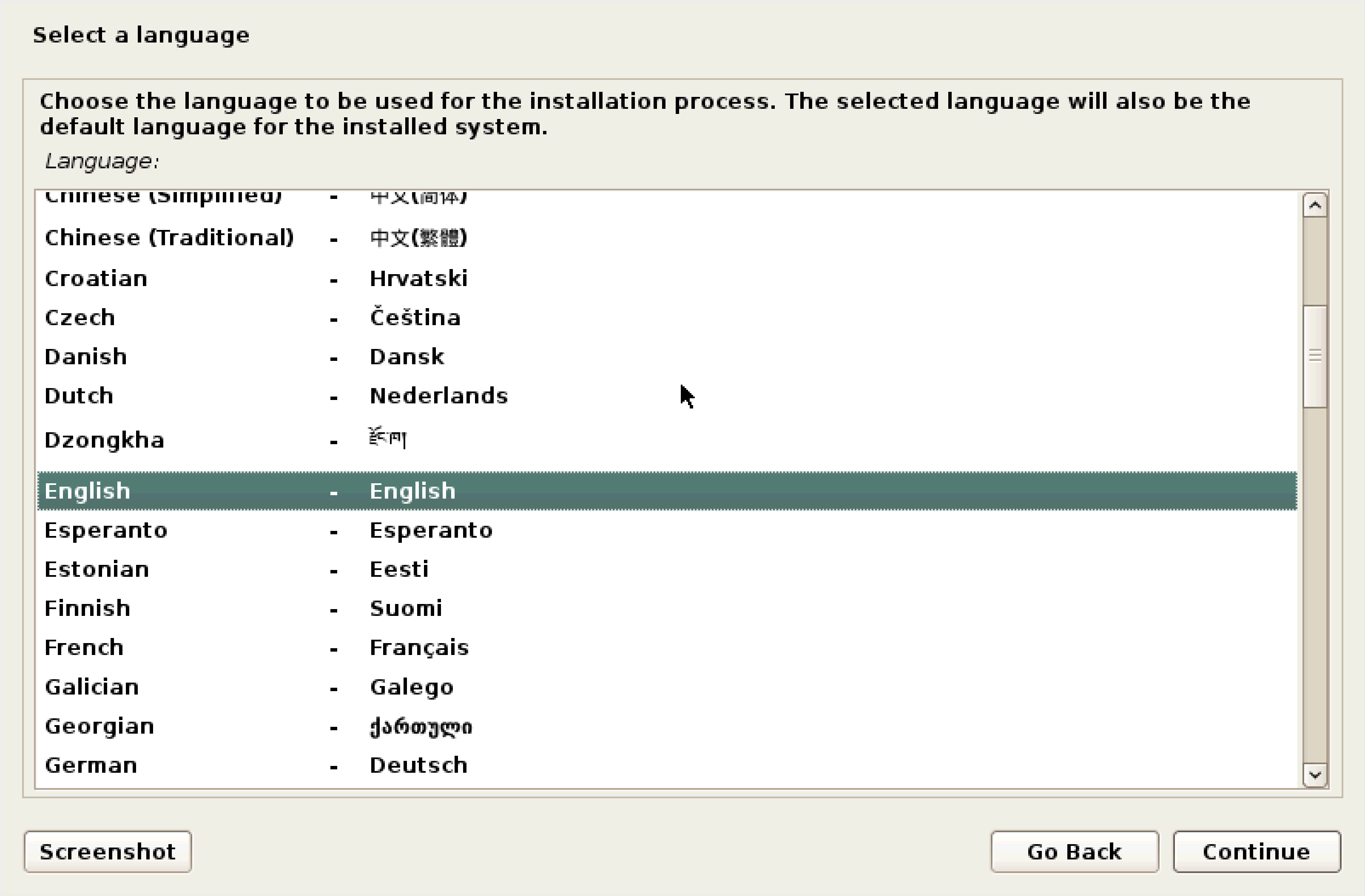


```
                    Boot menu

 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                                      >
```

The graphical installation mode looks like a wizard with multiple configuration screens.

Select a language.



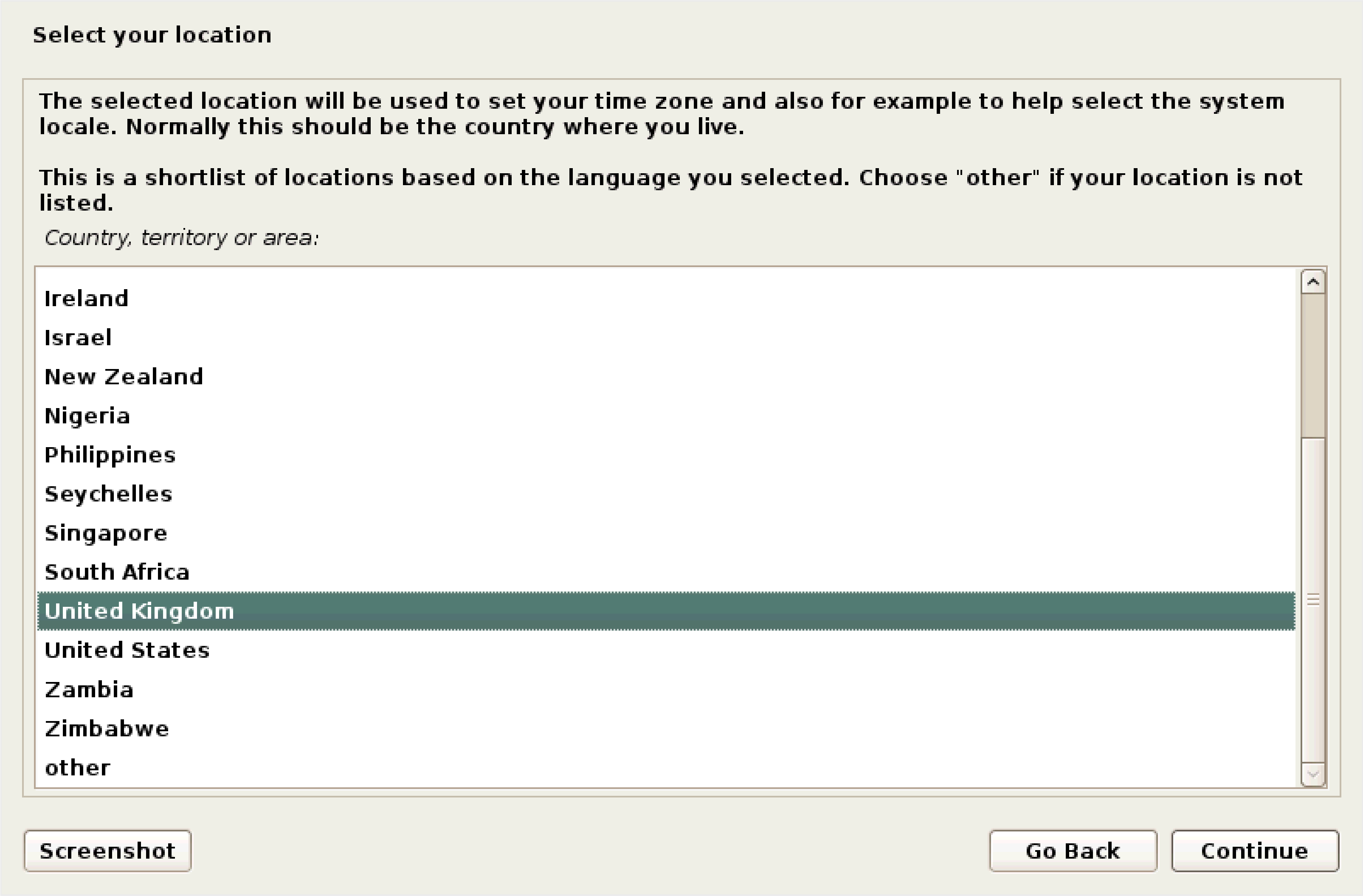
Select a language

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	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

Select your location.



Select your location

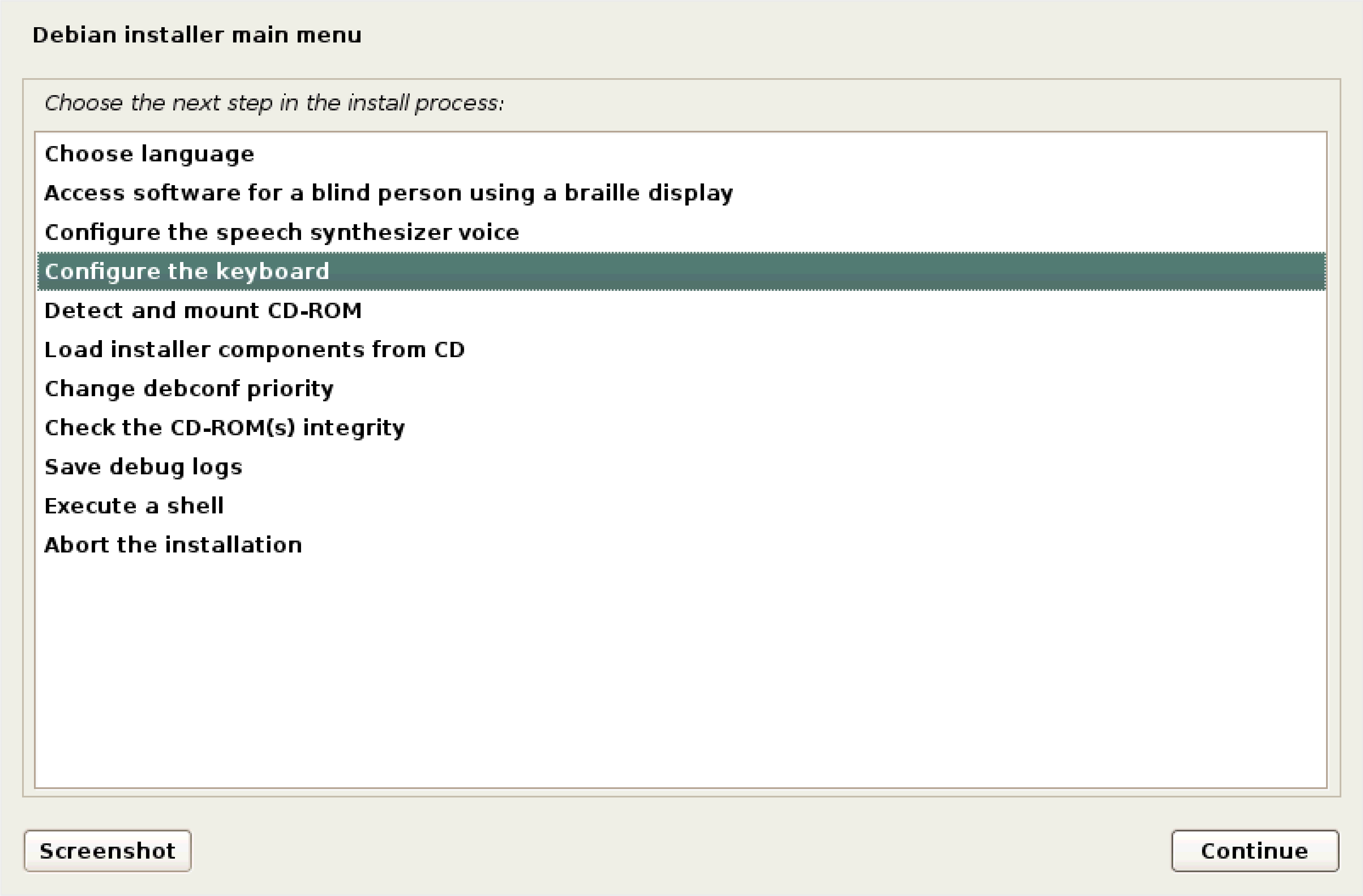
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

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

Country, territory or area:

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

Configure a keyboard.

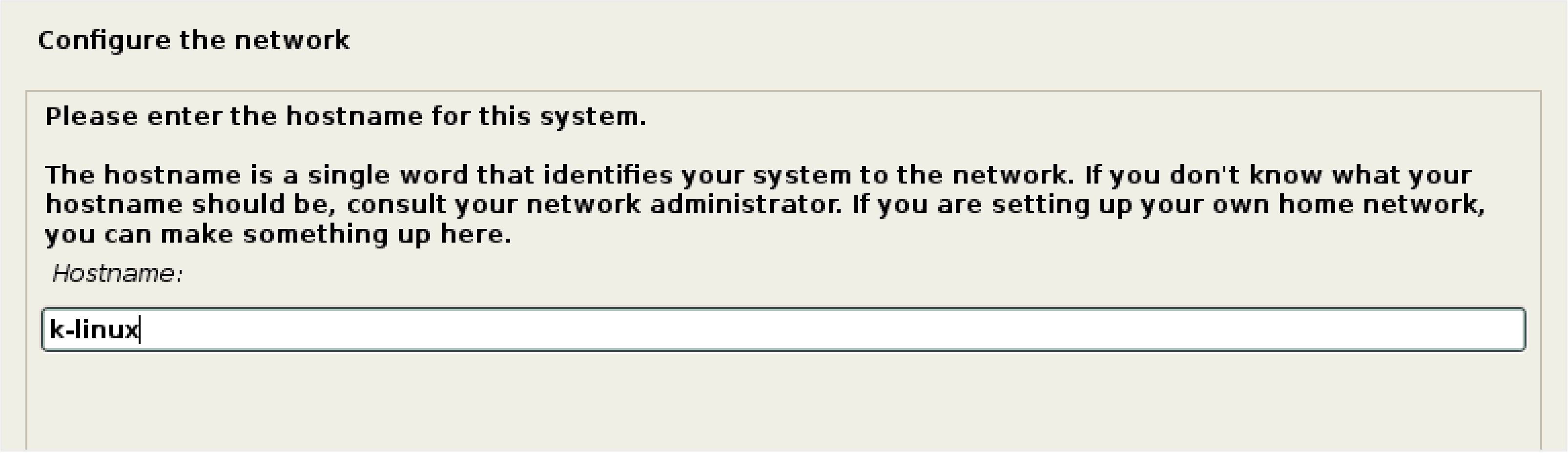


Debian installer main menu

Choose the next step in the install process:

- Choose language
- Access software for a blind person using a braille display
- Configure the speech synthesizer voice
- **Configure the keyboard**
- Detect and mount CD-ROM
- Load installer components from CD
- Change debconf priority
- Check the CD-ROM(s) integrity
- Save debug logs
- Execute a shell
- Abort the installation

Enter the hostname for this system, for example, *k-linux*.



Configure the network

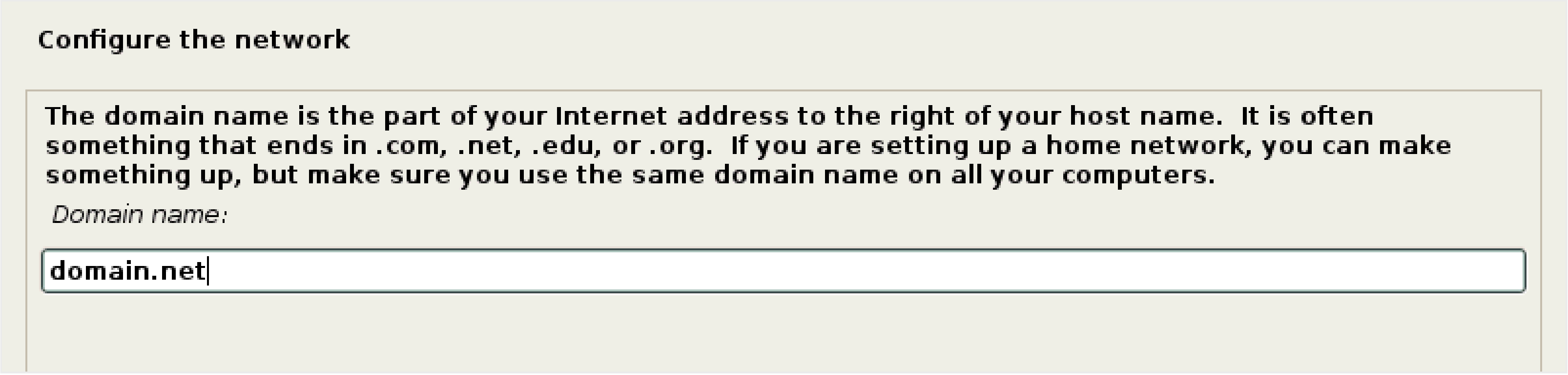
Please enter the hostname for this system.

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:

k-linux

Set the domain name, for example, *domain.net*.



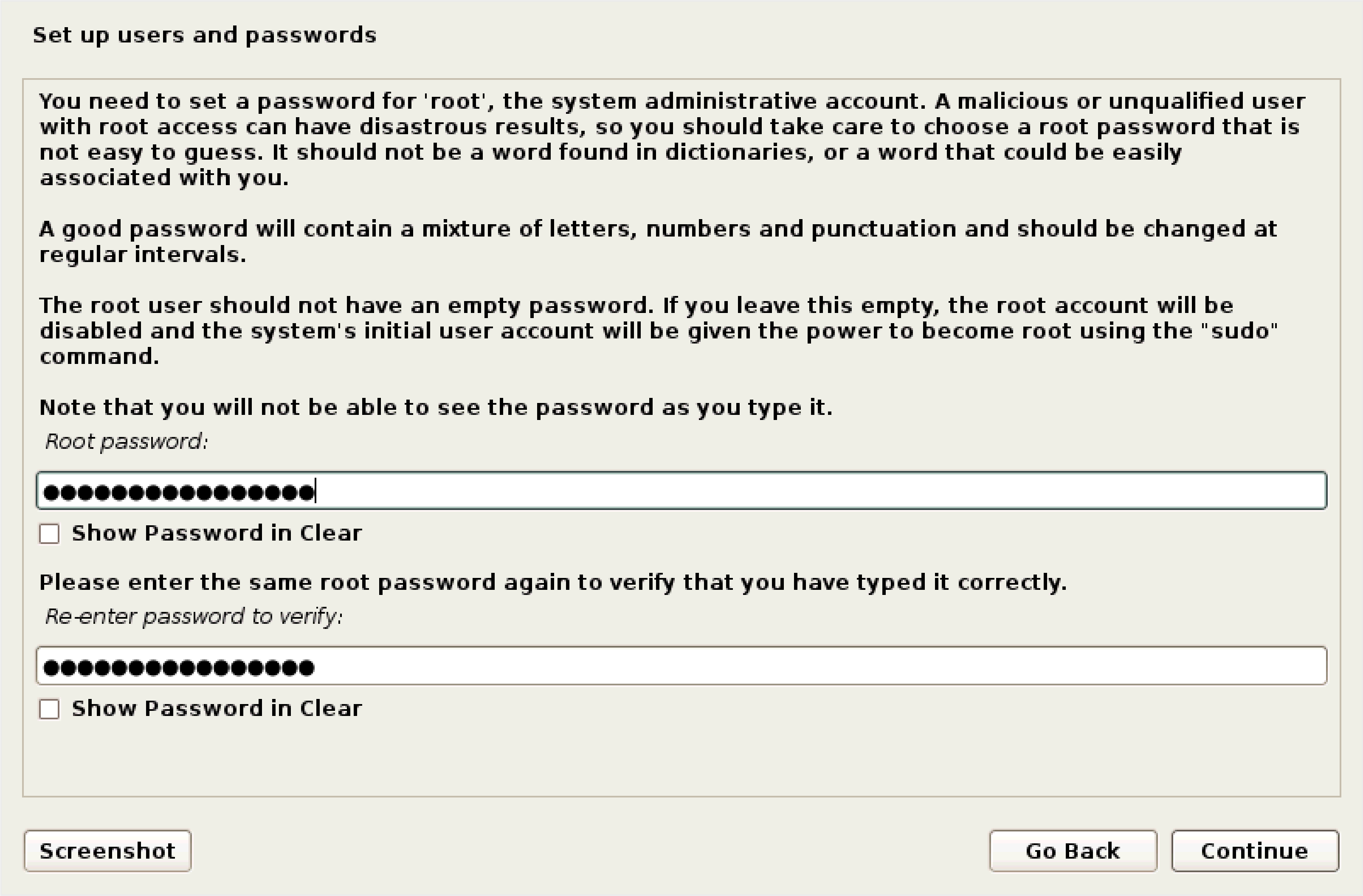
Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

domain.net

Set up the password for root user. Note that in some distributions of Kali Linux "toor" is the default password for the root user.



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

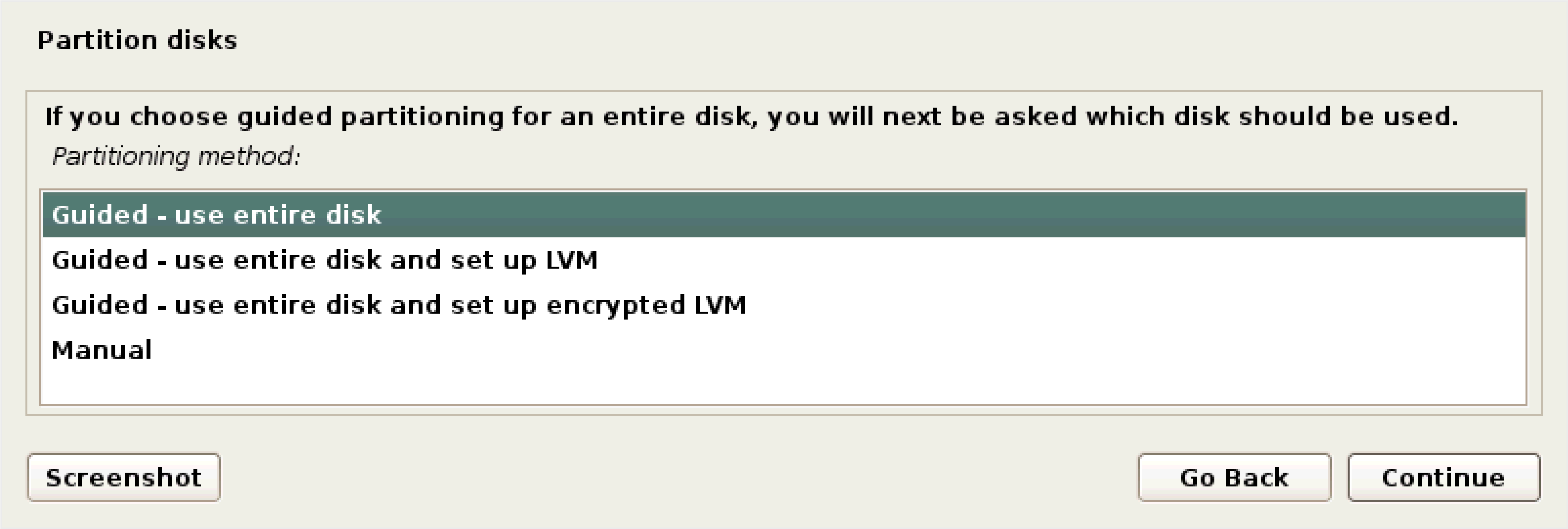
Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●●●●●●●●●●●

□ Show Password in Clear

Select the partitioning method for your disks. If you want to create a custom partitioning table, select **Manual**. Selecting **Guided – use entire disk** should be enough for the first time.



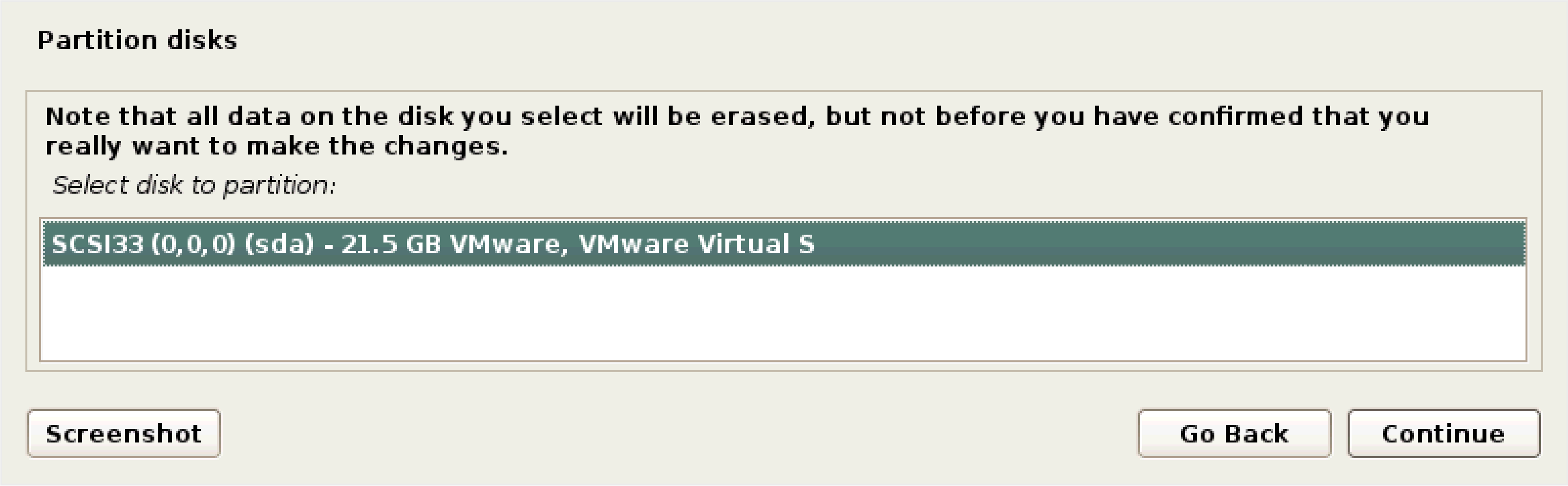
Partition disks

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

Select your virtual disk to be partitioned.



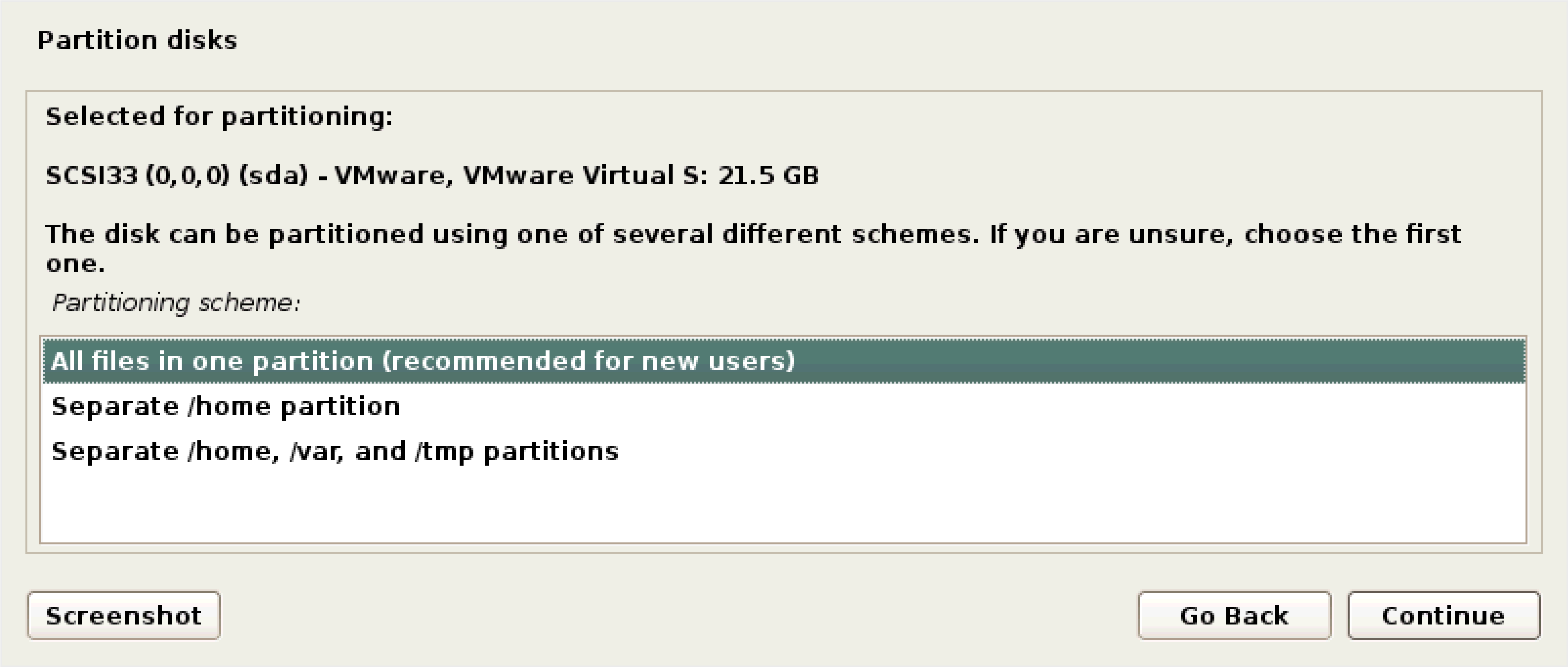
Partition disks

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:

- **SCSI33 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S**

Select **All files in one partition**.



Partition disks

Selected for partitioning:

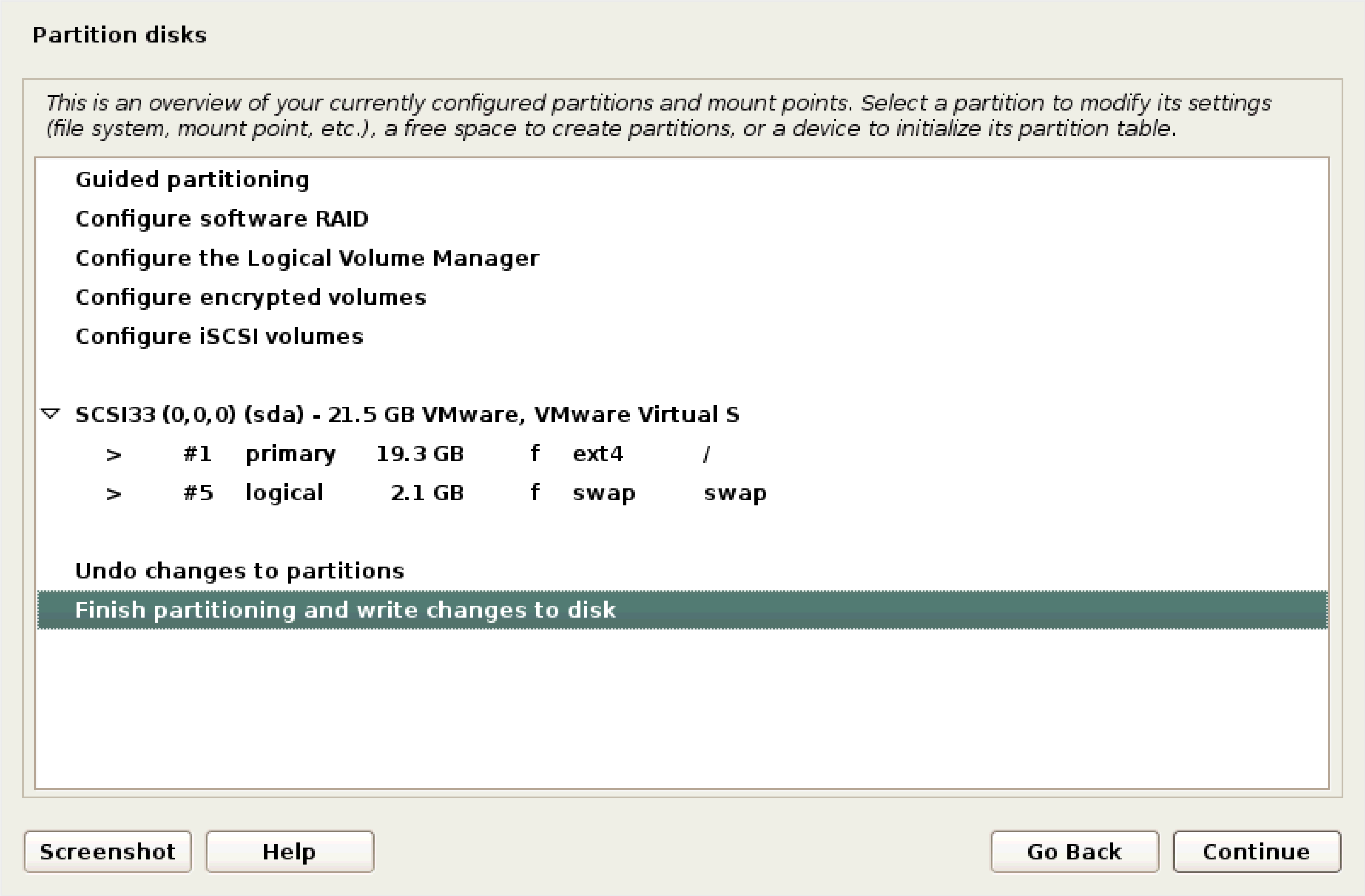
SCSI33 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB

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

Select **Finish partitioning and write changes to disk.**



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

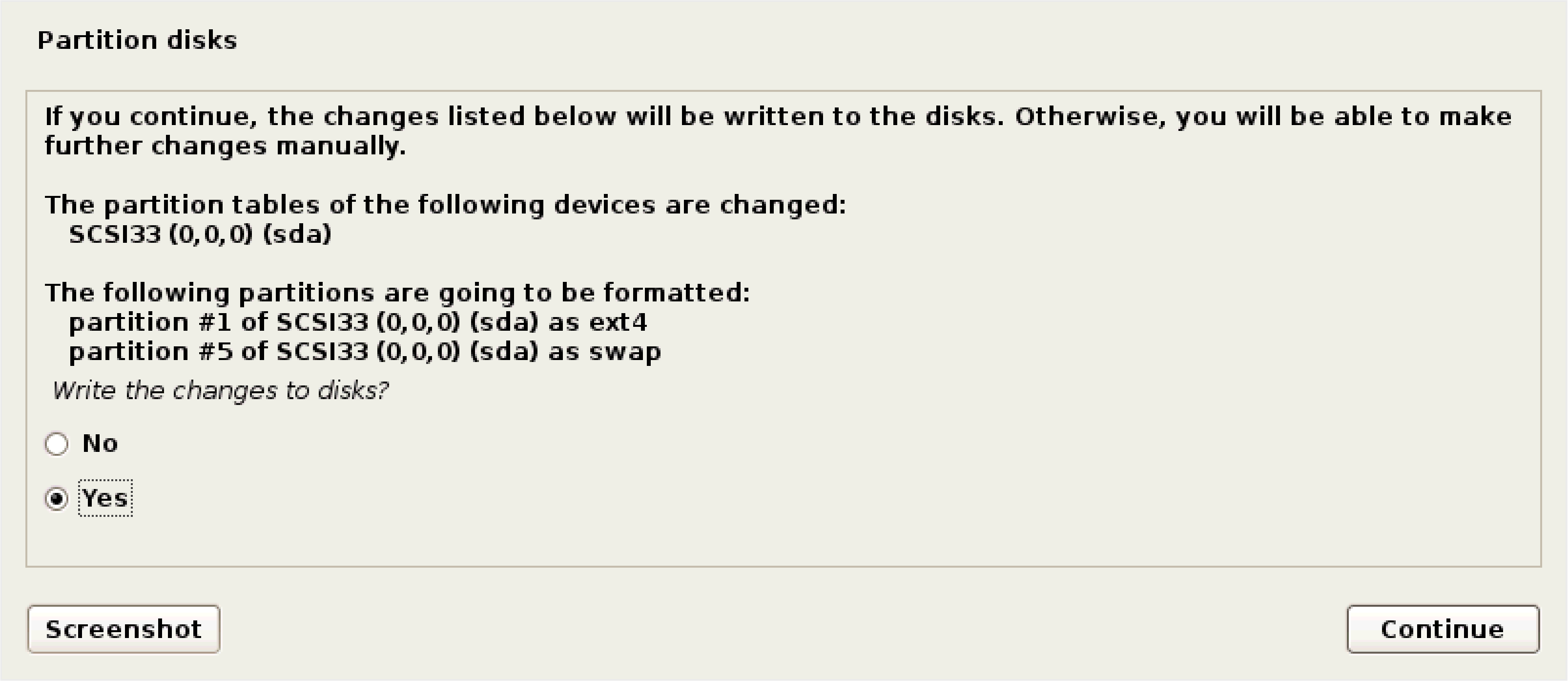
Configure iSCSI volumes

```
▽ SCSI33 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
     >     #1   primary    19.3 GB     f   ext4       /
     >     #5   logical     2.1 GB     f   swap       swap
```

Undo changes to partitions

Finish partitioning and write changes to disk

Click **Yes** to confirm creation of a new empty partition table on the virtual disk for writing changes to disk.



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:
  SCSI33 (0,0,0) (sda)

The following partitions are going to be formatted:
  partition #1 of SCSI33 (0,0,0) (sda) as ext4
  partition #5 of SCSI33 (0,0,0) (sda) as swap

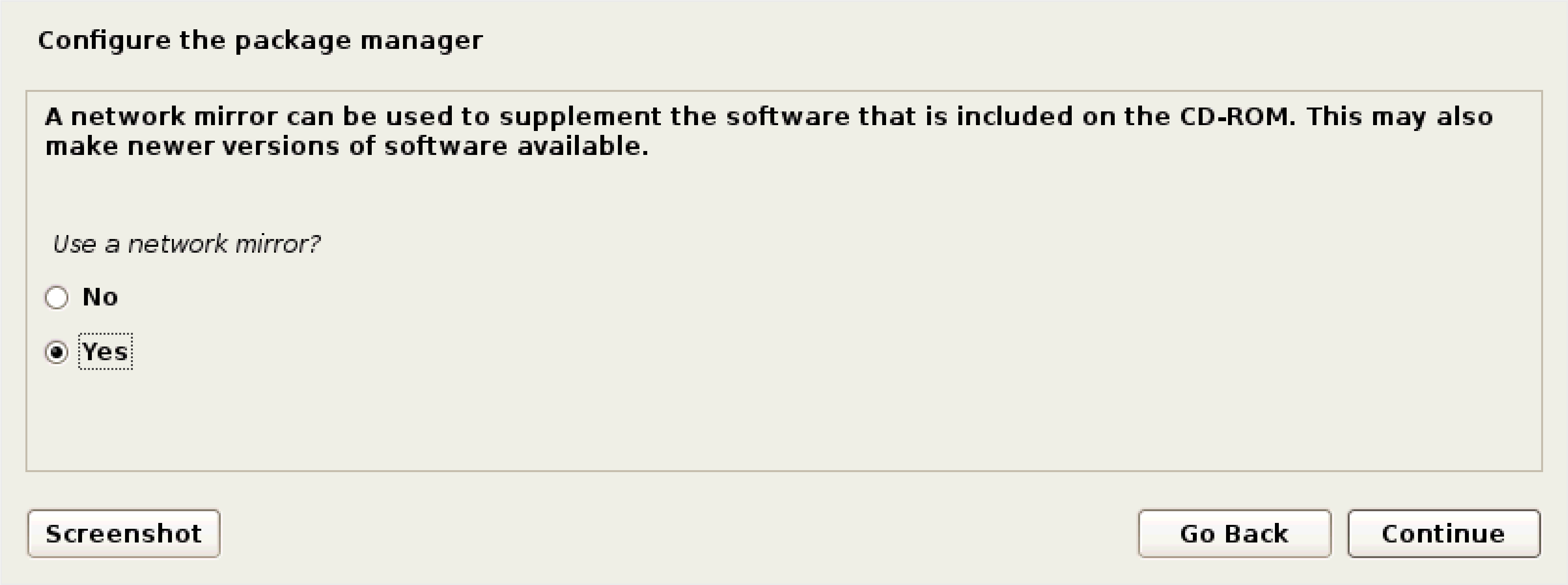
Write the changes to disks?

○ No

● Yes

The installation process starts after disk partitioning. Wait until the system installation is finished.

Configure the package manager. Select **Yes** to use a network mirror.



Configure the package manager

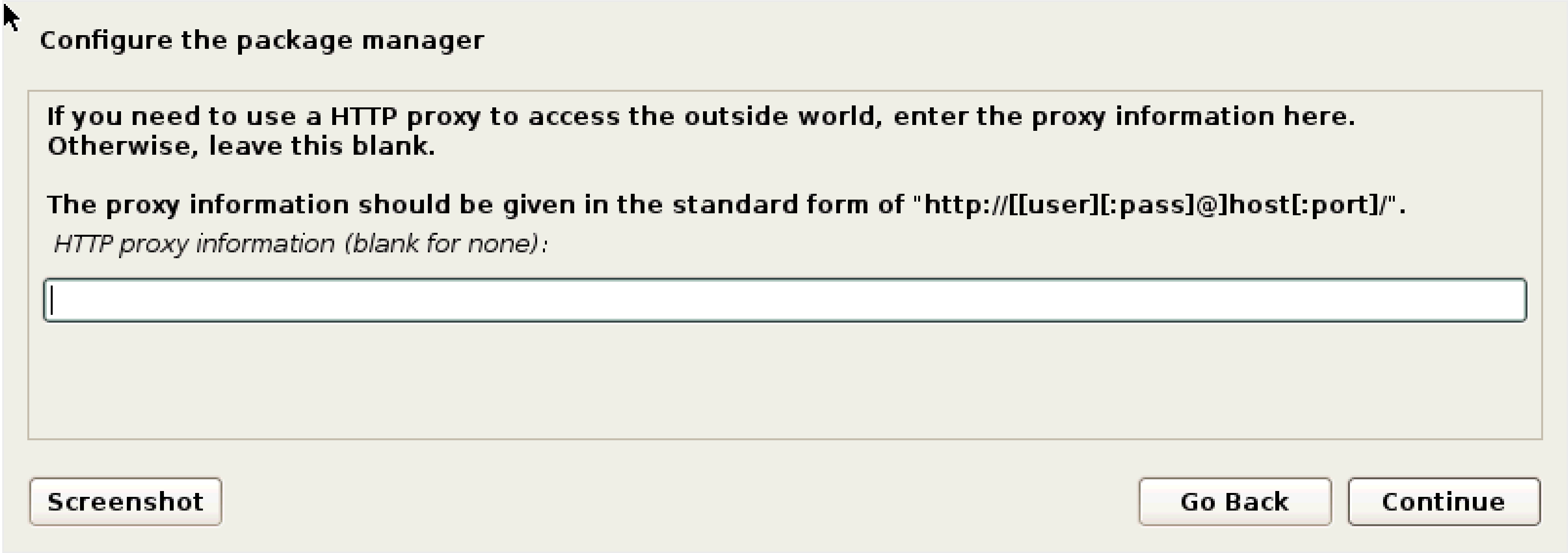
A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

○ No

● Yes

If you don’t have an HTTP proxy to access the outside networks, leave the field empty and click **Continue**.



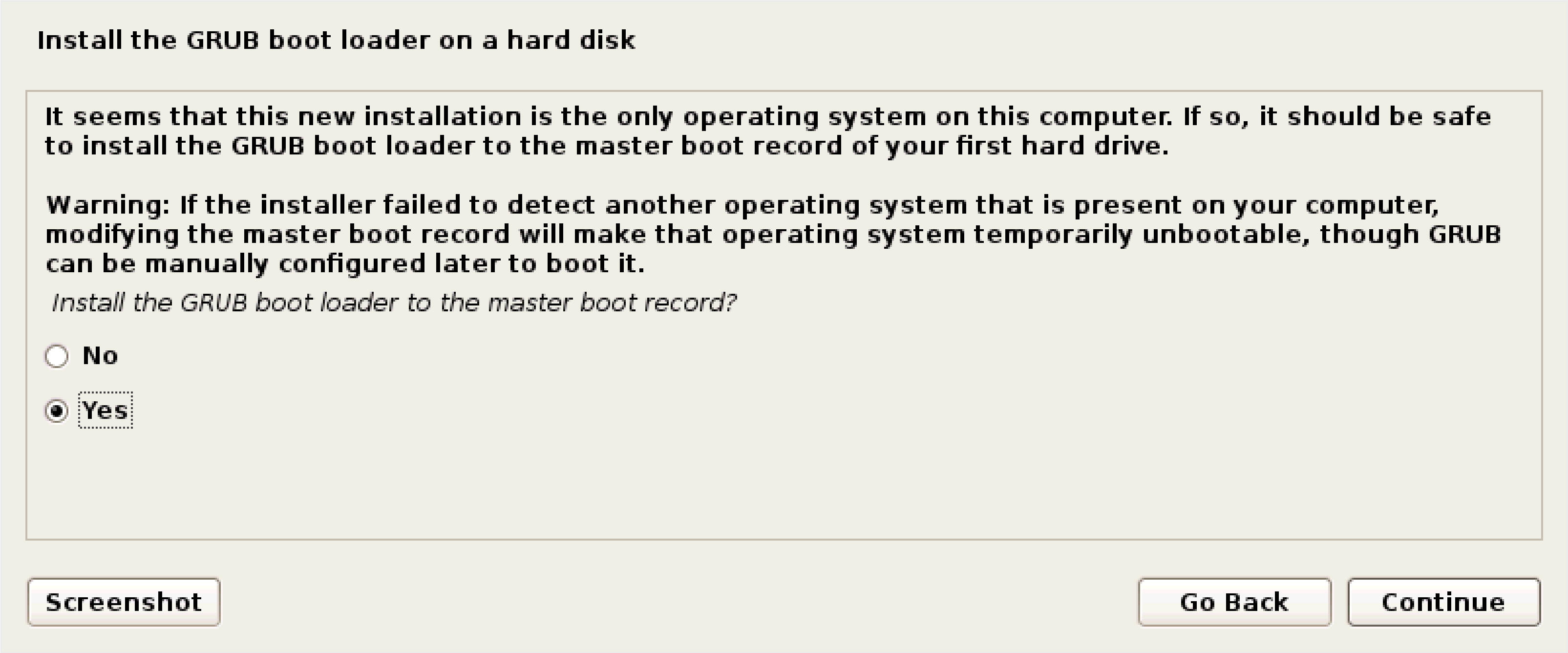
Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

Install the GRUB boot loader on a hard disk – click **Yes** to do this.



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.

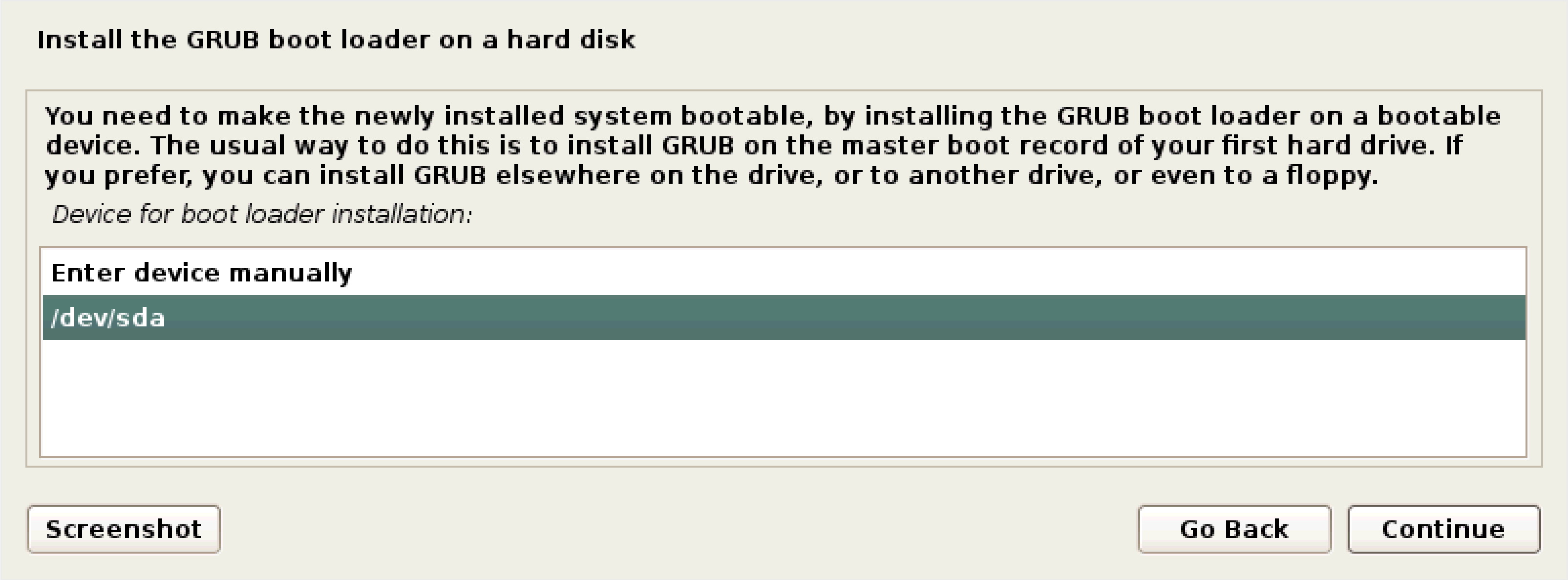
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

○ No

● Yes

Define the device for boot loader installation. We use **/dev/sda**.



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

Installation is complete. After rebooting your VM, enter *root* as the user name and enter the password you have specified during OS installation.

Installing VMware Tools on Kali Linux VMware VM

Now you have to install VMware Tools, i.e. a set of useful drivers and utilities that improves VM performance and interaction between host and guest (shared clipboard, drag & drop files, USB devices pass-through, etc.).

Make sure that Kali Linux VMware VM installed is running and click **VM > Install VMware Tools** in the menu bar or the VMware Workstation window. The ISO CD image is now inserted to the virtual CD/DVD drive of the VM. You can see the disc icon on the desktop of the guest OS. Open the terminal (**Applications > Terminal Emulator**).

Go to the directory of the inserted disc that contains VMware Tools by typing:

```
cd /media/cdrom
```

Create a directory on your desktop for extracting files from the archive to that directory.

```
mkdir ~/Desktop/VMwareTools
```

Extract VMware Tools installation files from the archive by using the following command:

```
tar -xvzf VMwareTools-10.3.2-9925305.tar.gz -C ~/Desktop/VMwareTools/
```

where:

tar is the Linux archiver application; **x** – tells tar to extract files; **v** – allows the verbose mode to see the output in console; **z** – tells tar to decompress files from an archive using gzip; **f** – defines a location of the compressed archive, files from which must be extracted.

Go to the directory where the files have been extracted.

```
cd ~/Desktop/VMwareTools/vmware-tools-distrib
```

Run the installer of VMware Tools:

```
./vmware-install.pl
```

Answer the questions provided by the console installation wizard. Press **Enter** to use the default values that are shown in [brackets]. When the installation process of VMware Tools is finished, reboot the VM by typing **init 6** in the terminal window.

Note: If you have an Internet connection, you can install VMware Tools with your **apt-get** Linux package manager by typing in the terminal the following command:

apt-get install open-vm-tools-desktop

Answer the questions provided by the installation wizard as mentioned before.

Configuring Screen Resolution

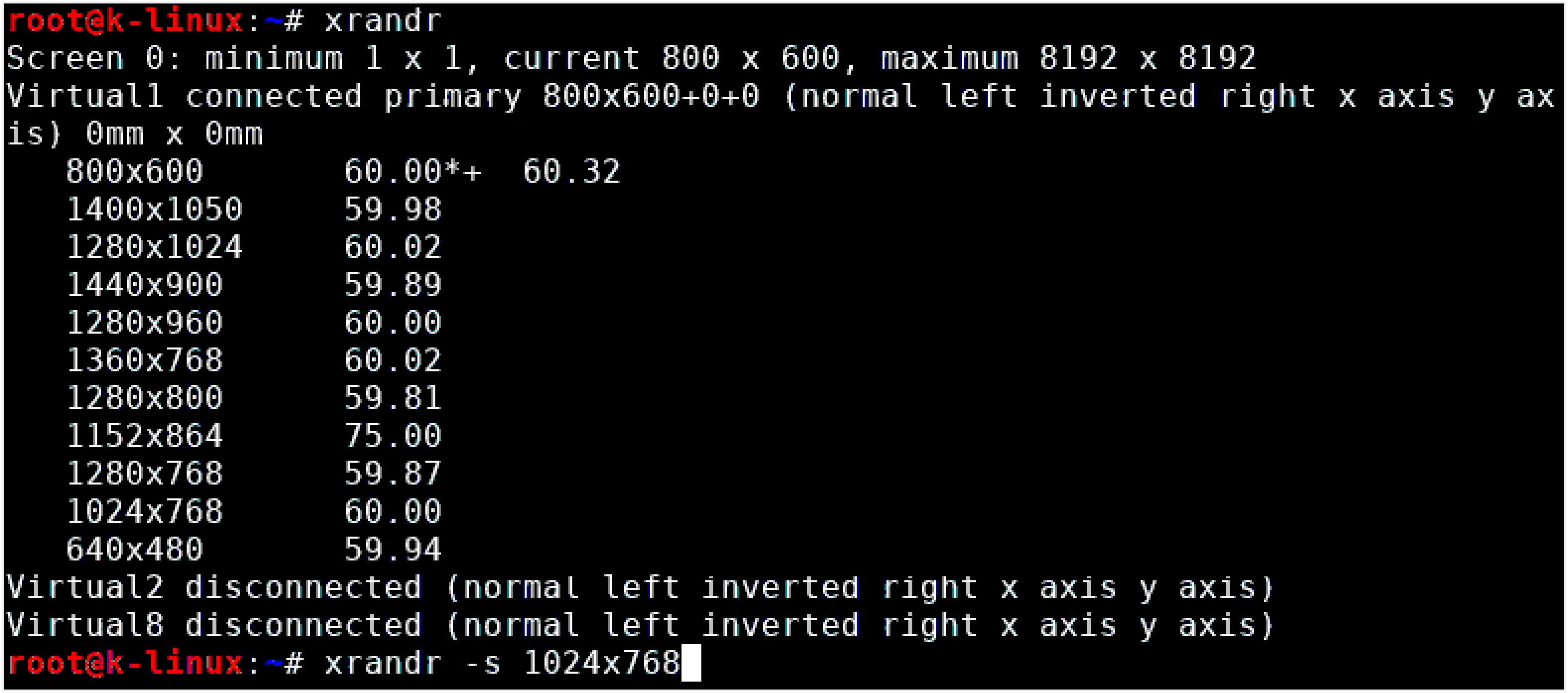
After installing VMware Tools on Kali Linux VMware VM, you can customize the screen resolution of the guest VM window.

Open the terminal.

Type **xrandr** to view available display modes. The current display mode is marked with the asterisk (*).

Set the custom resolution, for example, 1024x768, instead of the default resolution (800x600):

xrandr -s 1024x768



```
root@k-linux:~# xrandr
Screen 0: minimum 1 x 1, current 800 x 600, maximum 8192 x 8192
Virtual1 connected primary 800x600+0+0 (normal left inverted right x axis y ax
is) 0mm x 0mm
   800x600       60.00*+  60.32
   1400x1050     59.98
   1280x1024     60.02
   1440x900      59.89
   1280x960      60.00
   1360x768      60.02
   1280x800      59.81
   1152x864      75.00
   1280x768      59.87
   1024x768      60.00
   640x480       59.94
Virtual2 disconnected (normal left inverted right x axis y axis)
Virtual8 disconnected (normal left inverted right x axis y axis)
root@k-linux:~# xrandr -s 1024x768
```

You can also use GUI. Right click the empty space on your VM desktop, go to **Applications > Settings > Display**. Change resolution in the drop-down menu, click **Apply** and **Close**.

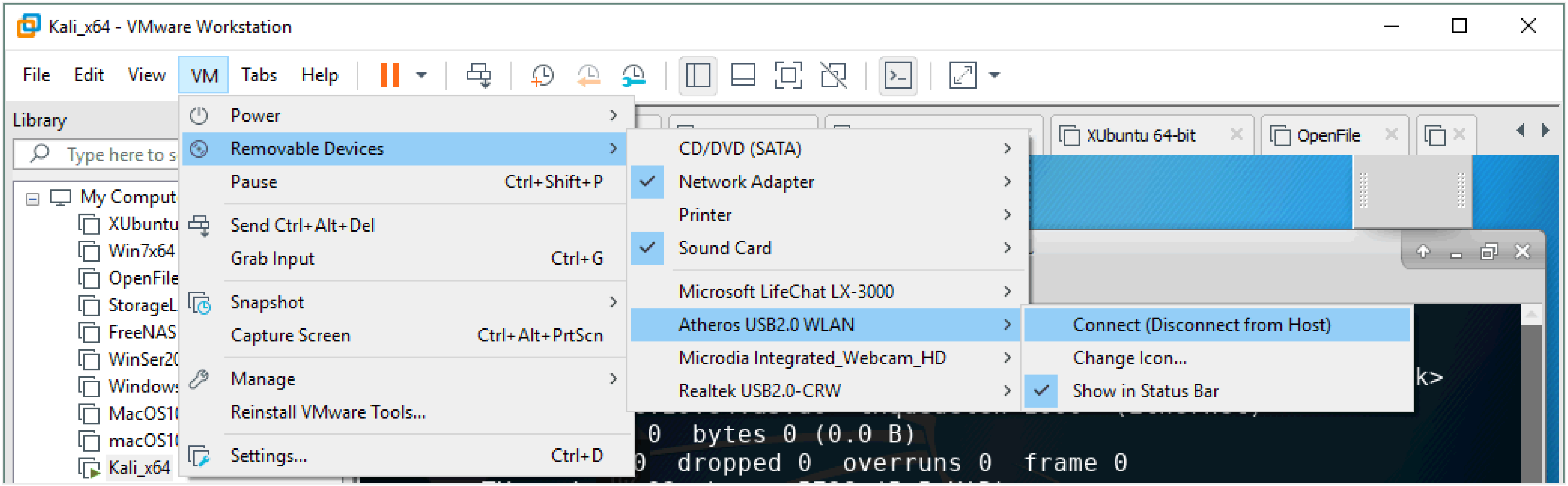
You can also enter a full screen mode of your Kali Linux VMware VM by clicking the **Full Screen** button in the VMware Workstation interface.

How to Connect a WI-FI Adapter to a VMware VM to Be Used by Kali Linux?

If you want to test Wi-Fi networks, then you need a Wi-Fi network adapter connected to a machine on which Kali Linux is running. It is not possible to connect a built-in wireless network adapter (that is usually connected with a PCI Express interface) of a laptop directly to a virtual machine. In this case, you can only use a bridged network mode, but low level adapter features such as entering to a monitor mode will be disabled. If you use a built-in wireless network adapter in the bridged network mode, a guest OS (Kali Linux in our example) identifies the network adapter as an emulated Ethernet adapter.

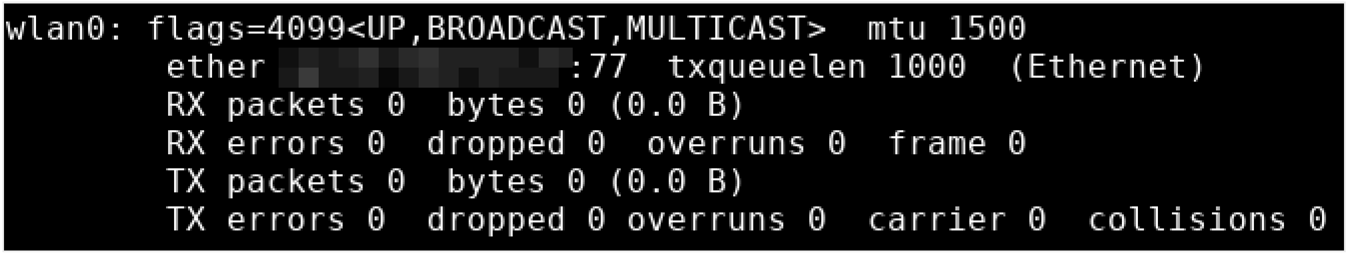
As you recall, VMware Workstation and ESXi server provide you with the ability to connect USB devices to a VM in the pass-through mode. In this mode a USB device is attached to a VM similarly as it would be attached to a physical machine. When you attach a USB device to a VM, it is disconnected from a host machine. A USB Wi-Fi adapter is what you need in this situation.

Get the external USB Wi-Fi adapter and insert it into a USB port of your host machine (a machine on which VMware Workstation is installed). Make sure that your Kali VM is running. Don't connect to any Wi-Fi networks on a host machine. In the VMware Workstation window go to **VM > Removable devices > [Your USB Wi-Fi adapter name] > Connect (Disconnect from host)**.



```
0  bytes 0 (0.0 B)
0  dropped 0  overruns 0  frame 0
```

Type **ifconfig** to check that your USB Wi-Fi adapter is detected by Kali Linux on VMware VM. In our example a wireless adapter is detected and its network interface is named **wlan0**.



```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether [redacted]:77  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Turn off the wireless network interface:

ifconfig wlan0 down

Change the MAC address of your wireless network adapter to a custom MAC address, for example, FC:FC:48:0A:0B:FF.

macchanger -m fc:fc:48:0a:0b:ff wlan0

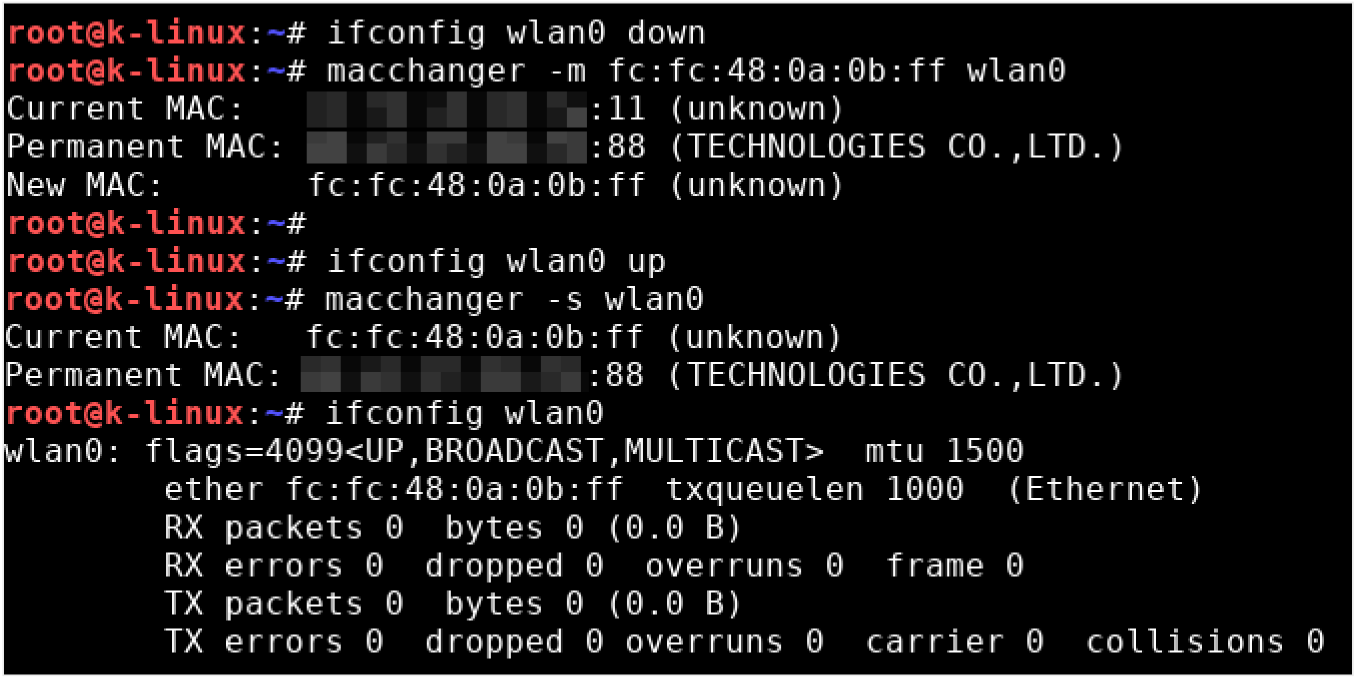
Turn on your wireless network interface.

ifconfig wlan0 up

Check whether the MAC address of your Wi-Fi adapter has been changed by using one of the following commands:

macchanger -s wlan0

ifconfig wlan0



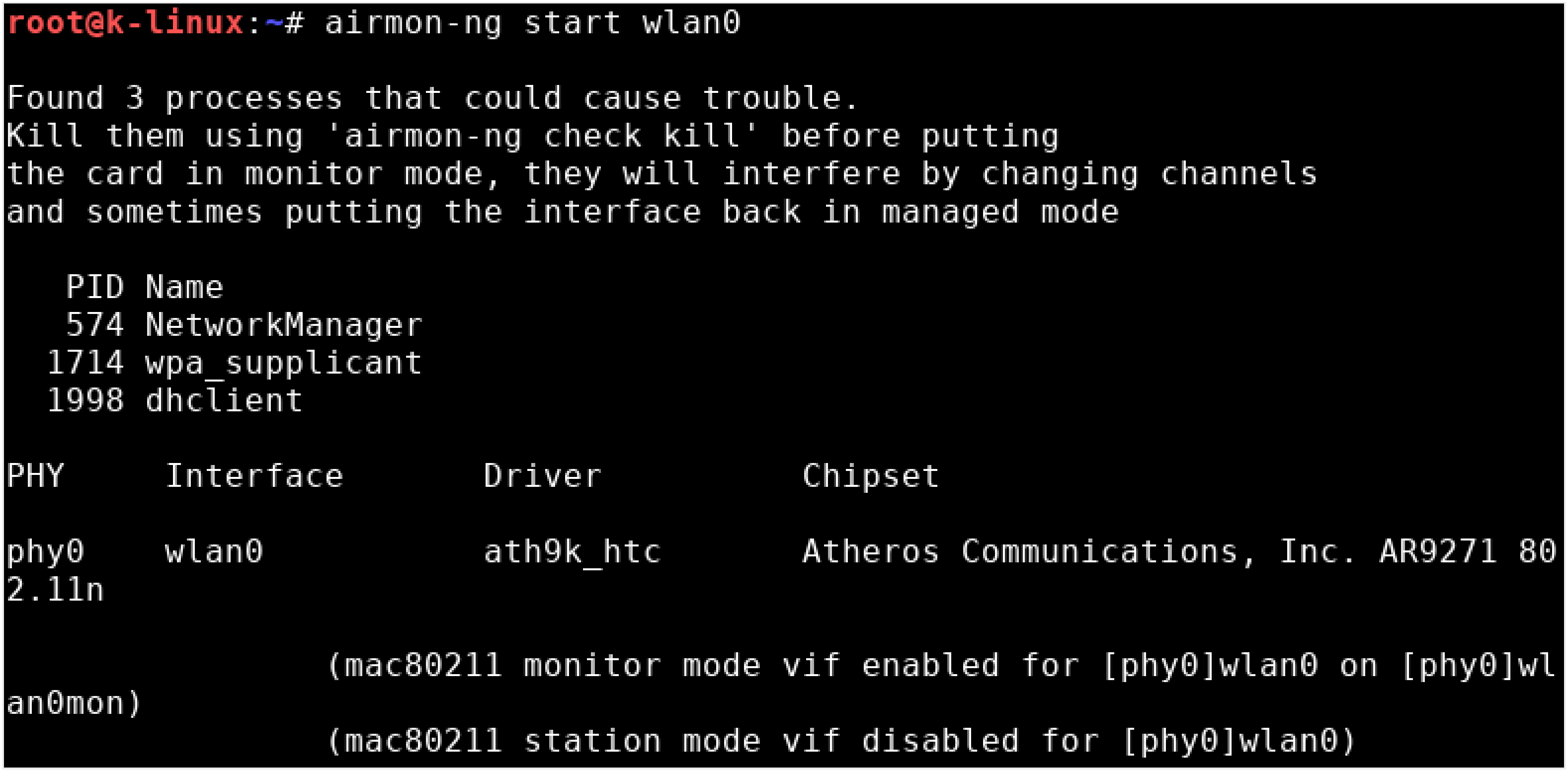
```
root@k-linux:~# ifconfig wlan0 down
root@k-linux:~# macchanger -m fc:fc:48:0a:0b:ff wlan0
Current MAC:   [redacted]:11 (unknown)
Permanent MAC: [redacted]:88 (TECHNOLOGIES CO.,LTD.)
New MAC:       fc:fc:48:0a:0b:ff (unknown)
root@k-linux:~#
root@k-linux:~# ifconfig wlan0 up
root@k-linux:~# macchanger -s wlan0
Current MAC:   fc:fc:48:0a:0b:ff (unknown)
Permanent MAC: [redacted]:88 (TECHNOLOGIES CO.,LTD.)
root@k-linux:~# ifconfig wlan0
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether fc:fc:48:0a:0b:ff  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

If the MAC address of your network adapter was not changed, check the sequence of commands you have run and try again. You can type **macchanger --help** to see a list of available options for using the *macchanger* tool.

After changing the MAC address, you can perform penetration testing and security auditing of Wi-Fi networks.

Switch the Wi-Fi network adapter into a monitor mode.

airmon-ng start wlan0



```
root@k-linux:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

   PID Name
   574 NetworkManager
  1714 wpa_supplicant
  1998 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 80
2.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wl
an0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

The **airmon-ng** utility notifies you if there are processes that could potentially cause trouble. It is recommended to kill such processes by typing the command:

airmon-ng check kill

You can additionally change the mac address of the **wlan0mon** interface.

ifconfig wlan0mon down

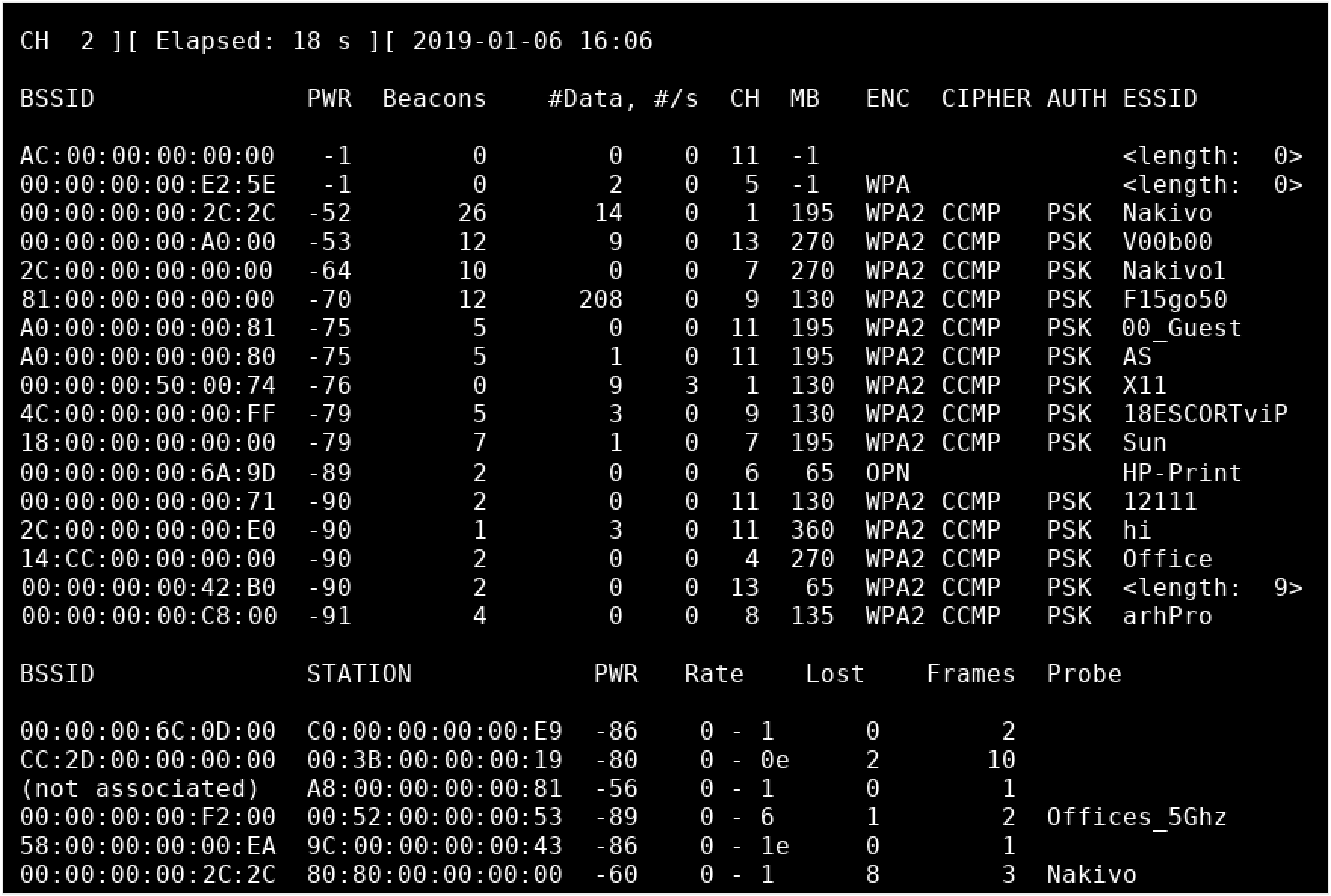
```
macchanger -m fc:fc:48:0a:0b:ff wlan0mon
```

```
ifconfig wlan0mon up
```

where **wlan0mon** is the name of the virtual monitoring network interface (formerly known as the **mon0** interface in BackTrack Linux).

Now you are ready to run the **airodump-ng** utility.

```
airodump-ng wlan0mon
```



```
CH  2 ][ Elapsed: 18 s ][ 2019-01-06 16:06

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

AC:00:00:00:00:00   -1        0        0    0  11  -1                    <length:  0>
00:00:00:00:E2:5E   -1        0        2    0   5  -1   WPA              <length:  0>
00:00:00:00:2C:2C  -52       26       14    0   1  195  WPA2 CCMP   PSK  Nakivo
00:00:00:00:A0:00  -53       12        9    0  13  270  WPA2 CCMP   PSK  V00b00
2C:00:00:00:00:00  -64       10        0    0   7  270  WPA2 CCMP   PSK  Nakivo1
81:00:00:00:00:00  -70       12      208    0   9  130  WPA2 CCMP   PSK  F15go50
A0:00:00:00:00:81  -75        5        0    0  11  195  WPA2 CCMP   PSK  00_Guest
A0:00:00:00:00:80  -75        5        1    0  11  195  WPA2 CCMP   PSK  AS
00:00:00:50:00:74  -76        0        9    3   1  130  WPA2 CCMP   PSK  X11
4C:00:00:00:00:FF  -79        5        3    0   9  130  WPA2 CCMP   PSK  18ESCORTviP
18:00:00:00:00:00  -79        7        1    0   7  195  WPA2 CCMP   PSK  Sun
00:00:00:00:6A:9D  -89        2        0    0   6   65  OPN              HP-Print
00:00:00:00:00:71  -90        2        0    0  11  130  WPA2 CCMP   PSK  12111
2C:00:00:00:00:E0  -90        1        3    0  11  360  WPA2 CCMP   PSK  hi
14:CC:00:00:00:00  -90        2        0    0   4  270  WPA2 CCMP   PSK  Office
00:00:00:00:42:B0  -90        2        0    0  13   65  WPA2 CCMP   PSK  <length:  9>
00:00:00:00:C8:00  -91        4        0    0   8  135  WPA2 CCMP   PSK  arhPro

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:00:00:6C:0D:00  C0:00:00:00:00:E9  -86    0 - 1      0        2
CC:2D:00:00:00:00  00:3B:00:00:00:19  -80    0 - 0e     2       10
(not associated)   A8:00:00:00:00:81  -56    0 - 1      0        1
00:00:00:00:F2:00  00:52:00:00:00:53  -89    0 - 6      1        2  Offices_5Ghz
58:00:00:00:00:EA  9C:00:00:00:00:43  -86    0 - 1e     0        1
00:00:00:00:2C:2C  80:80:00:00:00:00  -60    0 - 1      8        3  Nakivo
```

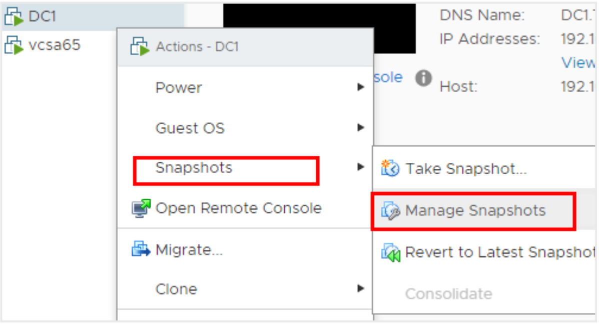
As you can see, the USB Wi-Fi adapter connected to the VM in the pass-through mode works fine. You can see access points and associated clients as well as capture wireless network packets for further analysis in the framework of network audit. Penetration testing and security audits are important but details of this process are out of the scope of this blog post. The emphasis of this article is that your Kali Linux deployed on an isolated VM can operate similarly as Kali Linux deployed on a physical machine.

Conclusion

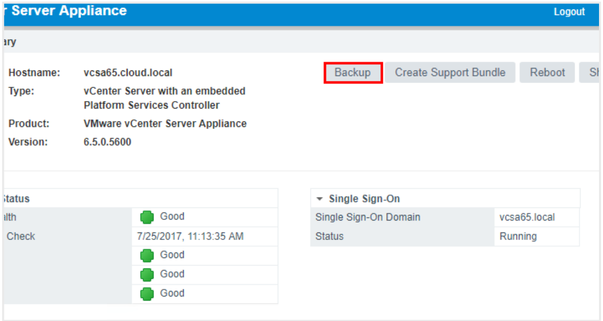
Kali Linux is a great Debian-based Linux distribution full of useful tools for penetration testing. Above, we have explored how to install Kali Linux on VMware Workstation VM. Creating a VM and the installation process of the operating system is not difficult, and a GUI provides useful understandable tips and comments. The key requirement is to configure a USB wireless network adapter connected to a VM by using a pass-through mode. This enables all hardware-based adapter's features from an isolated VM with Kali Linux for packet analyzing. Installing Kali Linux on an ESXi VM is similar to installing Kali on a VMware Workstation VM. You can also use VMware vCenter Converter to convert a VM of the Workstation format to a VM of the ESXi format.

4.5 (89.7%) 99 votes

People also read



[VMware Snapshots in vSphere How To]



Hostname: vcsa65.cloud.local
Type: vCenter Server with an embedded Platform Services Controller
Product: VMware vCenter Server Appliance
Version: 6.5.0.5600

tatus	
lth	🟩 Good
Check	7/25/2017, 11:13:35 AM
	🟩 Good
	🟩 Good
	🟩 Good

Single Sign-On	
Single Sign-On Domain	vcsa65.local
Status	Running

[Back Up a vCenter Server Appliance: How-To]

[How to Upgrade to VMware vCenter 7 and vSAN 7]

Older post

Newer post

Categories

Top Posts

Request Demo

Request a live demo by one of our engineers

Request Demo

Download Free Trial

Download a full-featured free trial

Download ↓

See Pricing

See the full list of features, editions and prices

See Pricing

Sales

Email: sales@nakivo.com
Fax: +1 408 516 9464

Support

Email: support@nakivo.com

Americas: +1 408 335 7367 (worldwide)
EMEA: +44 20 7097 1535
Taiwan: +886 2 7735 4556

Americas: +1 702 605 4495
Europe: +44 207 193 1230
Asia: +886 2 7735 4555

NAKIVO on social media:

Get special offers and updates:

Enter email address

SUBSCRIBE

Privacy Policy | EULA