# Setting up the CTF VM

## Step 0 - Prerequisites:

In order to play the CTF, you will need to have a Virtual Machine Manager installed. The setup script will work in Kali, which should be able to run in any Virtual Machine Manager. Some of the most popular Virtual Machine Managers include:

- Virtual Box [FREE] - https://www.virtualbox.org/wiki/Downloads

  > ⚠ **Warning**
  > DOES NOT WORK ON MACOS

- VMware Workstation Pro (Windows/Linux) or VMware Fusion (Mac OS) [FREE] - https://blogs.vmware.com/cloud-foundation/2024/05/13/vmware-workstation-pro-now-available-free-for-personal-use/
- MacOS Parallels [PAID only] - https://www.parallels.com/
- Virtual Manager, Gnome Boxes, etc. [LINUX only] - Install via your repo

> 🖉 **Note**
>
> If you already have a Kali VM set up, then you can skip down to **Step 2 - Install Kali** in these instructions.
> If you have a dedicated Kali installed on laptop (bare metal), then you can skip to **Step 3 - Run the setup script** in these instructions.

## VMWare Fusion

To ensure first-time CTF players have a working Virtual Machine Manager, we have provided the following instructions for VMware Fusion, which is free. You will need to register on the Broadcom website (they own VMware).

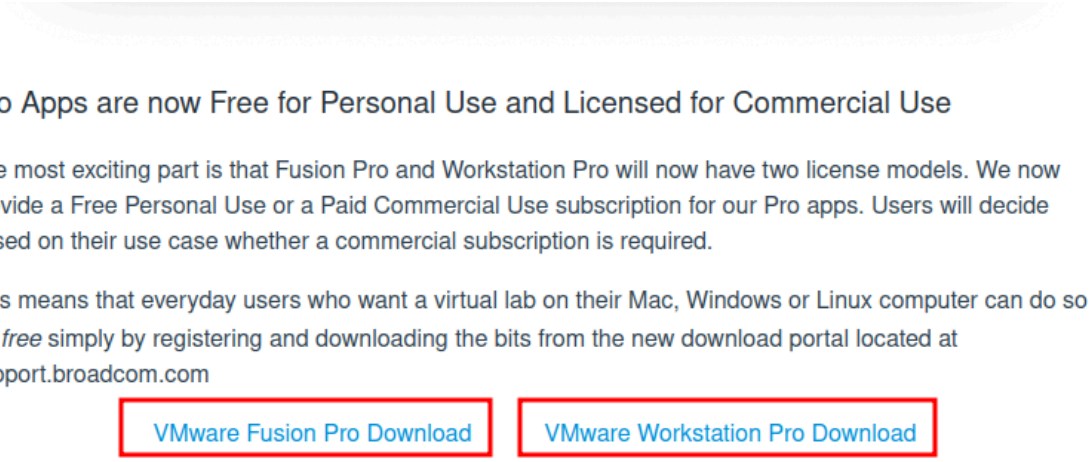
If you do not like providing your information to Broadcom, the only other options are not free.

> 🖉 **Note**
>
> If you already have a Kali VM set up, then you can skip down to **Step 2 - Install Kali** in these instructions.

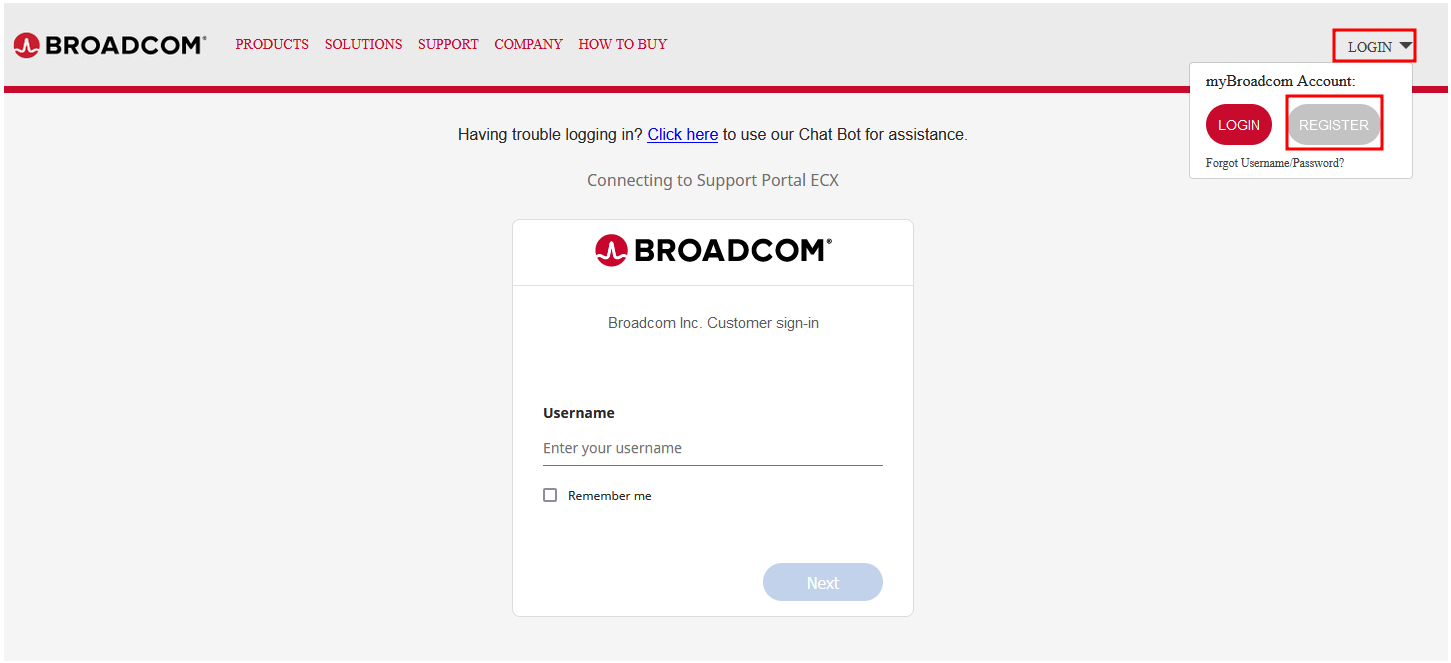
If you have a dedicated Kali installed on laptop (bare metal), then you can skip to **Step 3 - Run the setup script** in these instructions.

## To register with on the Broadcom site:

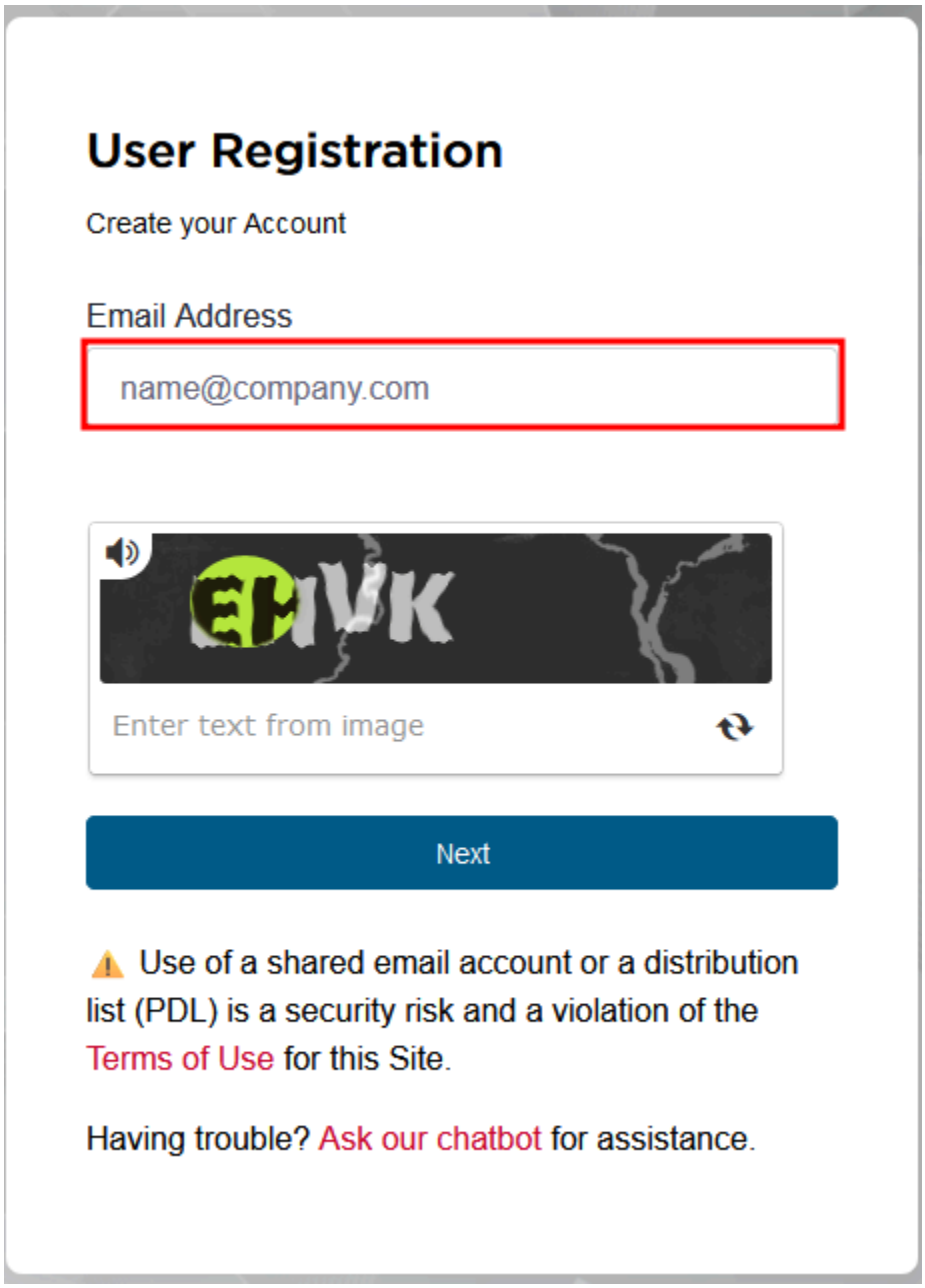
- Go to the following VMware site: https://blogs.vmware.com/teamfusion/2024/05/fusion-pro-now-available-free-for-personal-use.html
- Look for the download link for VMware Fusion (about 1/3 down the page) and click it:




- This will open up the Broadcom site for the download. If you don't already have an account, click the Login link in the upper right of the page, then select the register button:

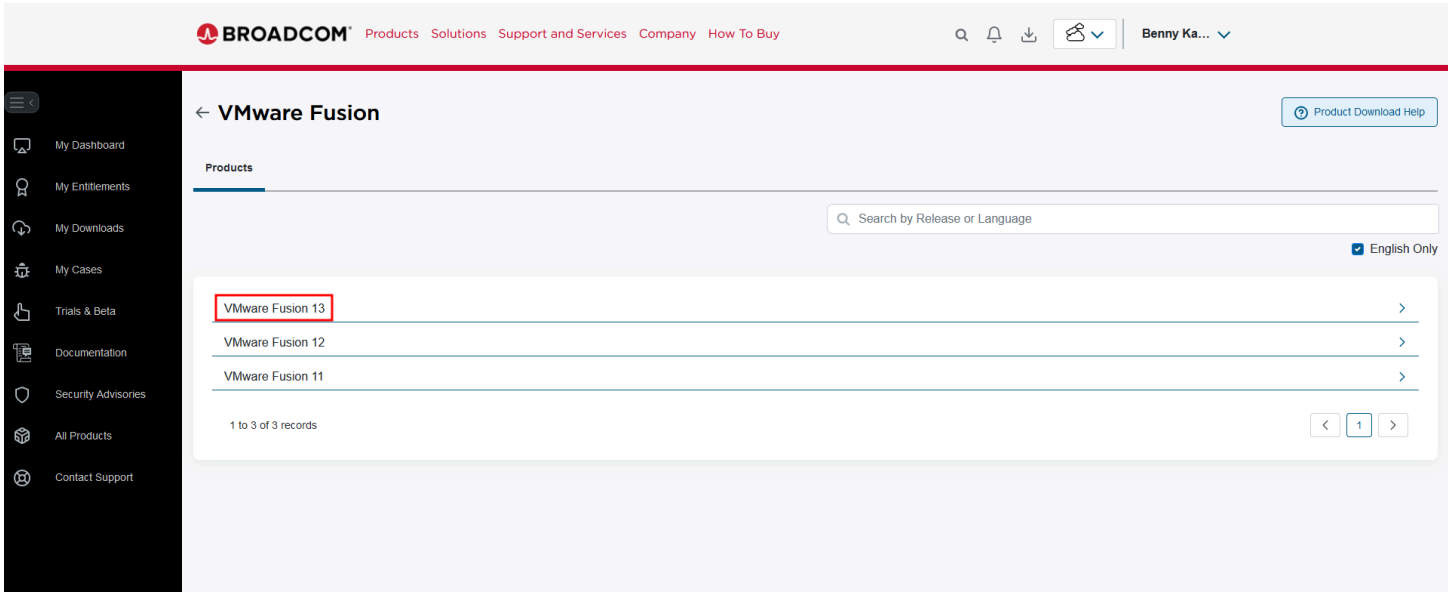


- On the User Registration page, enter your email:

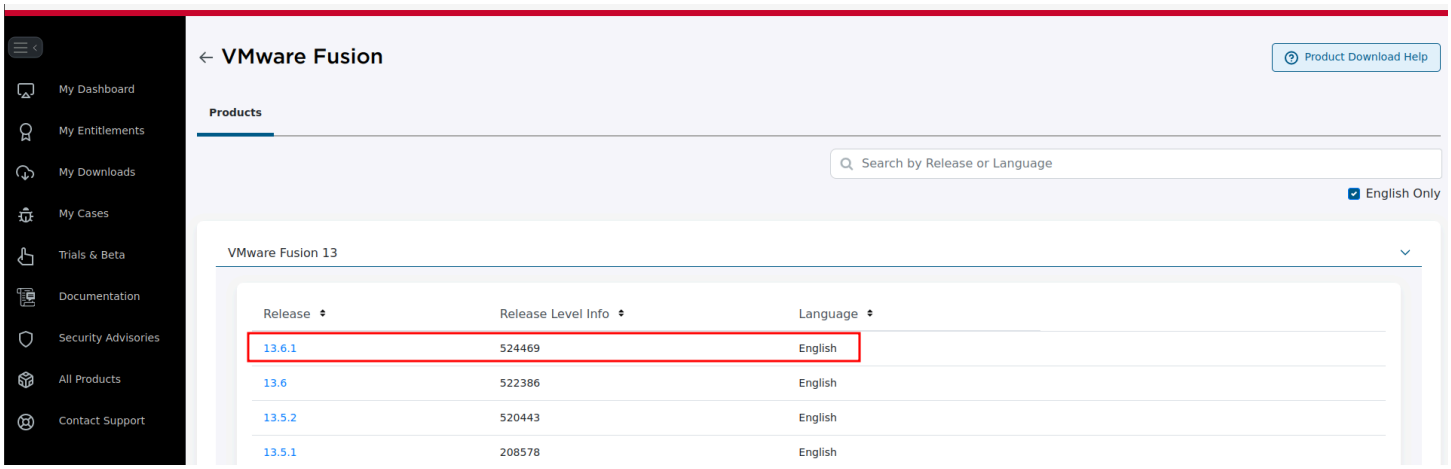



- You will then have to finish the user account. Once your account is created, then you can go and download the software.
- After logging into the Broadcom site, go to the Fusion Download page: https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware%20Fusion&freeDownloads=true

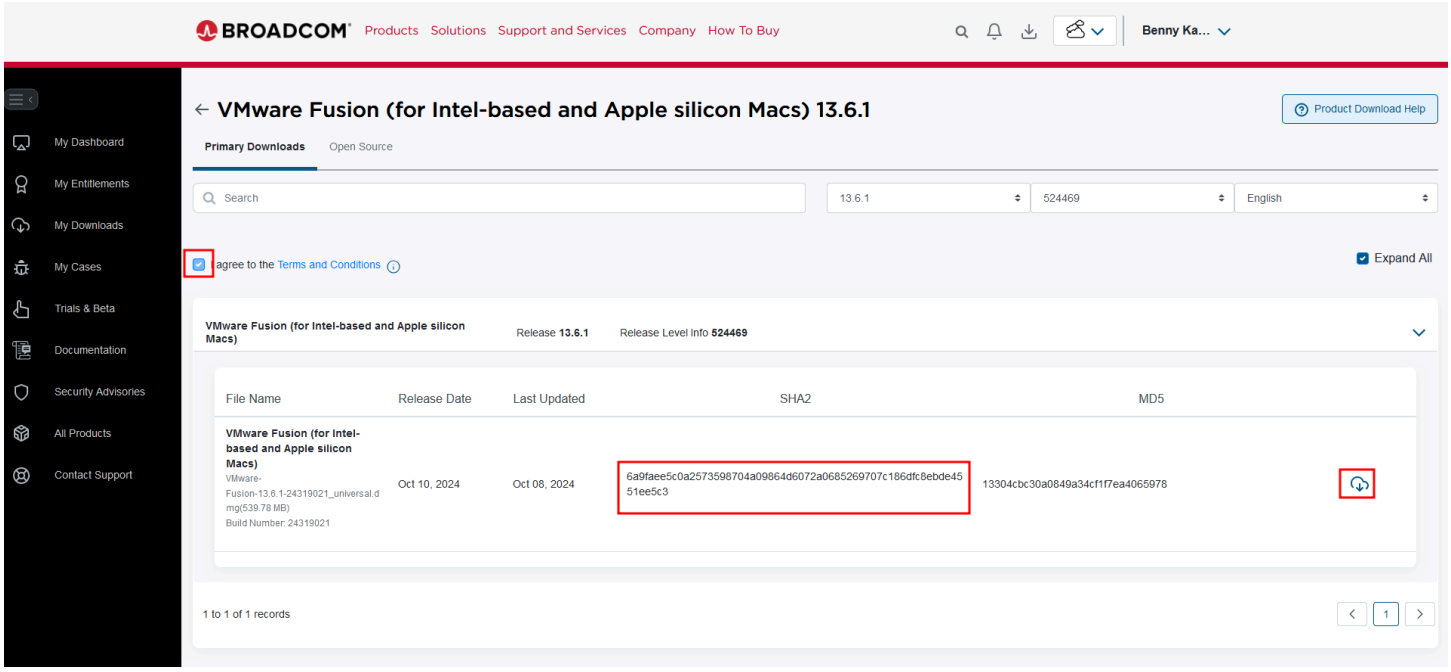
- Select VMware Fusion 13:




- Then, click on the latest release (which is 13.6.1 at the time of this documentation):




- Click on the I agree to the Terms and Conditions and then click on the Download button. Also, copy the SHA256 check sum for reference later.




# Step 1 - Install VMware Fusion:

- [ ] Download the required DMG file (from above)
- [ ] Do CheckSums for the DMG
    - If you are unsure how to do this, see the appendix below
- [ ] Install VMware normally (Next, next, etc.)
- [ ] You are now ready for **Step 2 - Install Kali**.

## Step 2 - Install Kali:

> **Fresh_Kali_Install_ISO-AppleSilicon-VMware**

# Kali inside VMware Fusion (Guest VM)

> **Note**
>
> For latest versions, see https://www.kali.org/get-kali/#kali-installer-images

This guide is about virtualizing Kali Linux inside of VirtualBox, allowing you to have a Kali VM. This is a great way to use Kali, as it is completely separate from the host, allows you to interact with other VMs (as well as the host machine and other machines on the network), and allows you to revert to snapshots.

You may wish to follow our other guide if you are trying to install VirtualBox on Kali Linux (as a host).

The guide below is what we use to generate our pre-made Kali Linux VirtualBox images. You may alter this to your needs. We always generate the images using the latest version of VirtualBox.

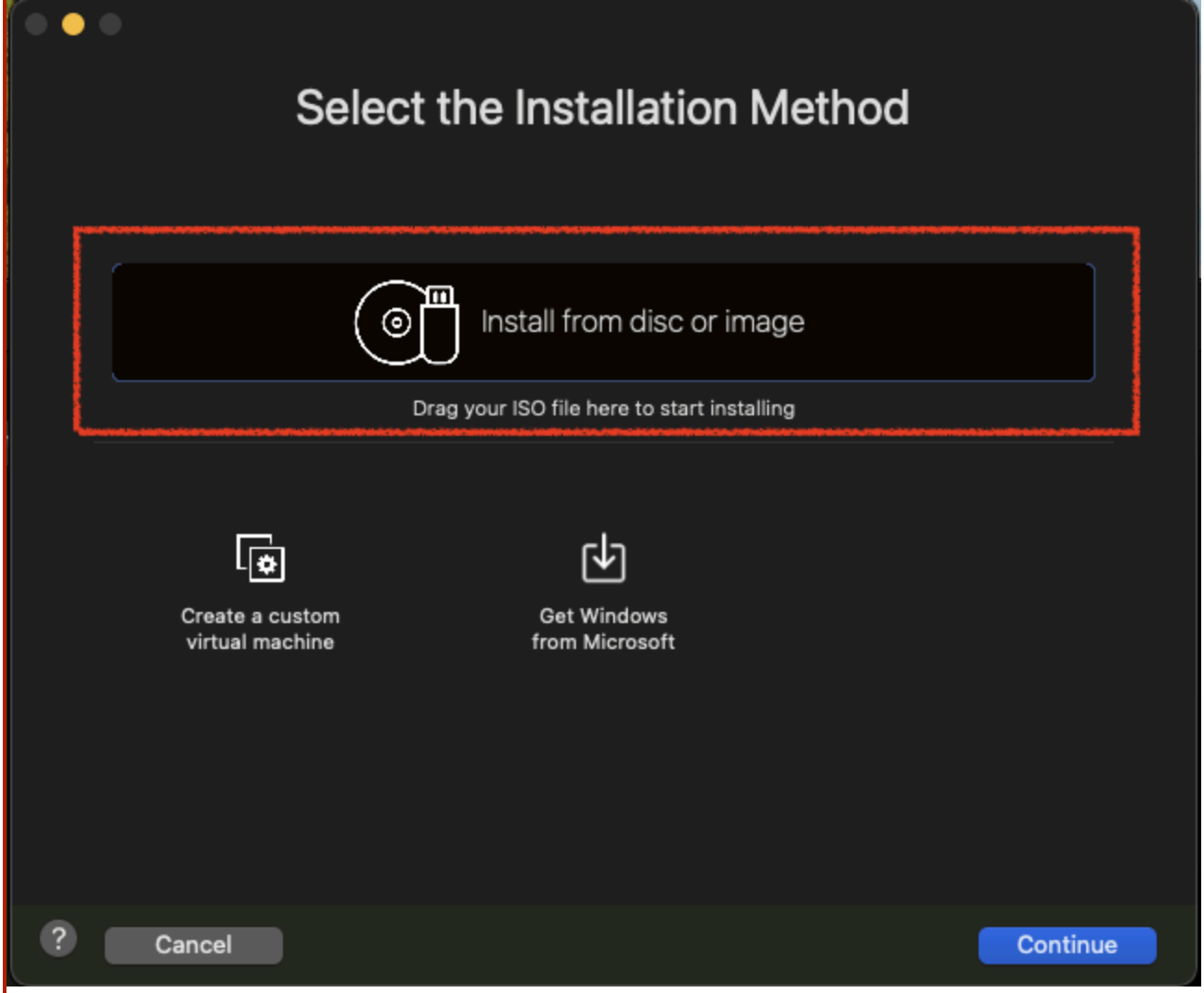
> **Note**
>
> You may need to enable virtualization in your BIOS/UEFI for (e.g. Intel VT-x/AMD-V)

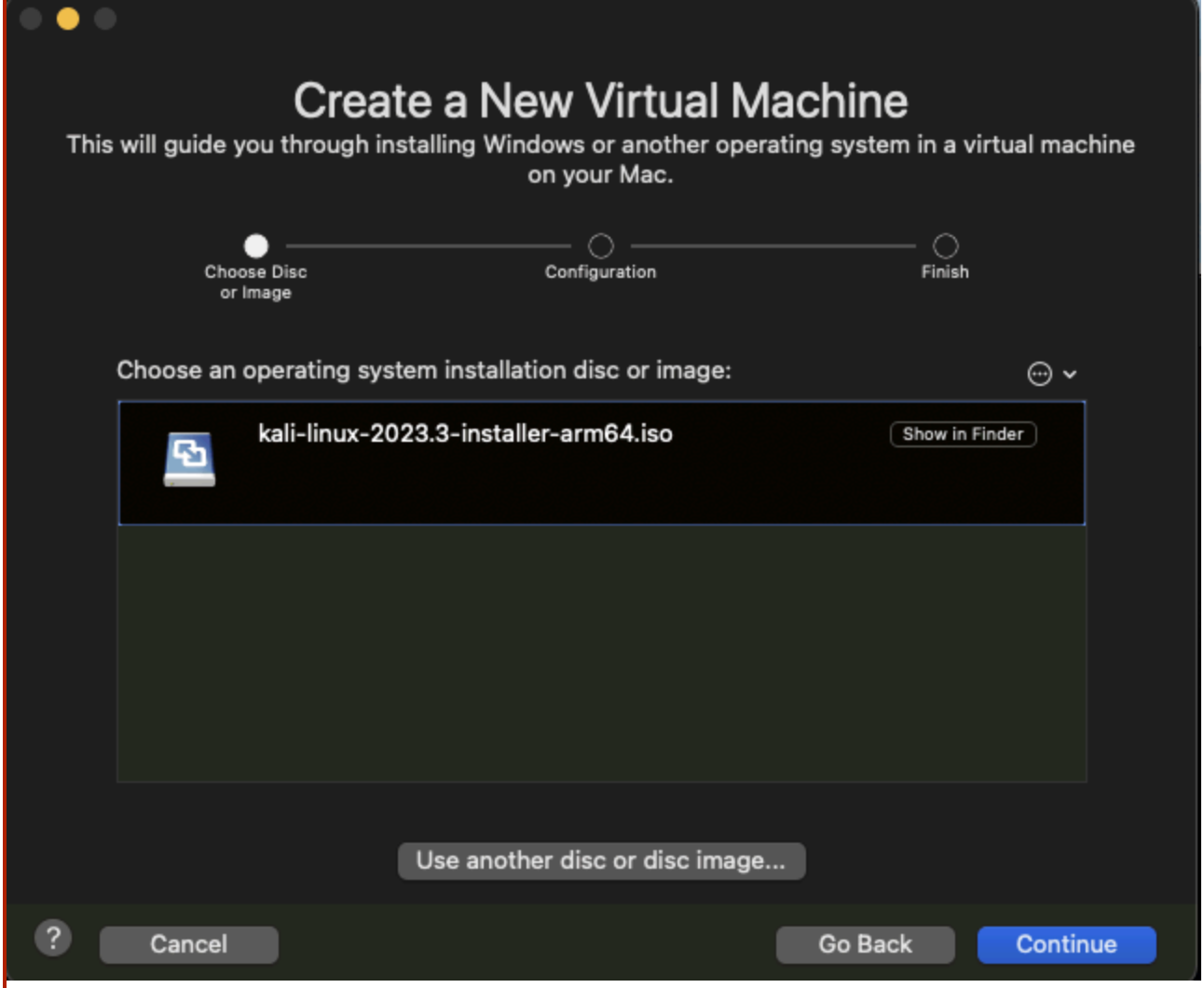
If you are on Apple Silicon, which is Arm64, then choose the Apple Silicon ISO:

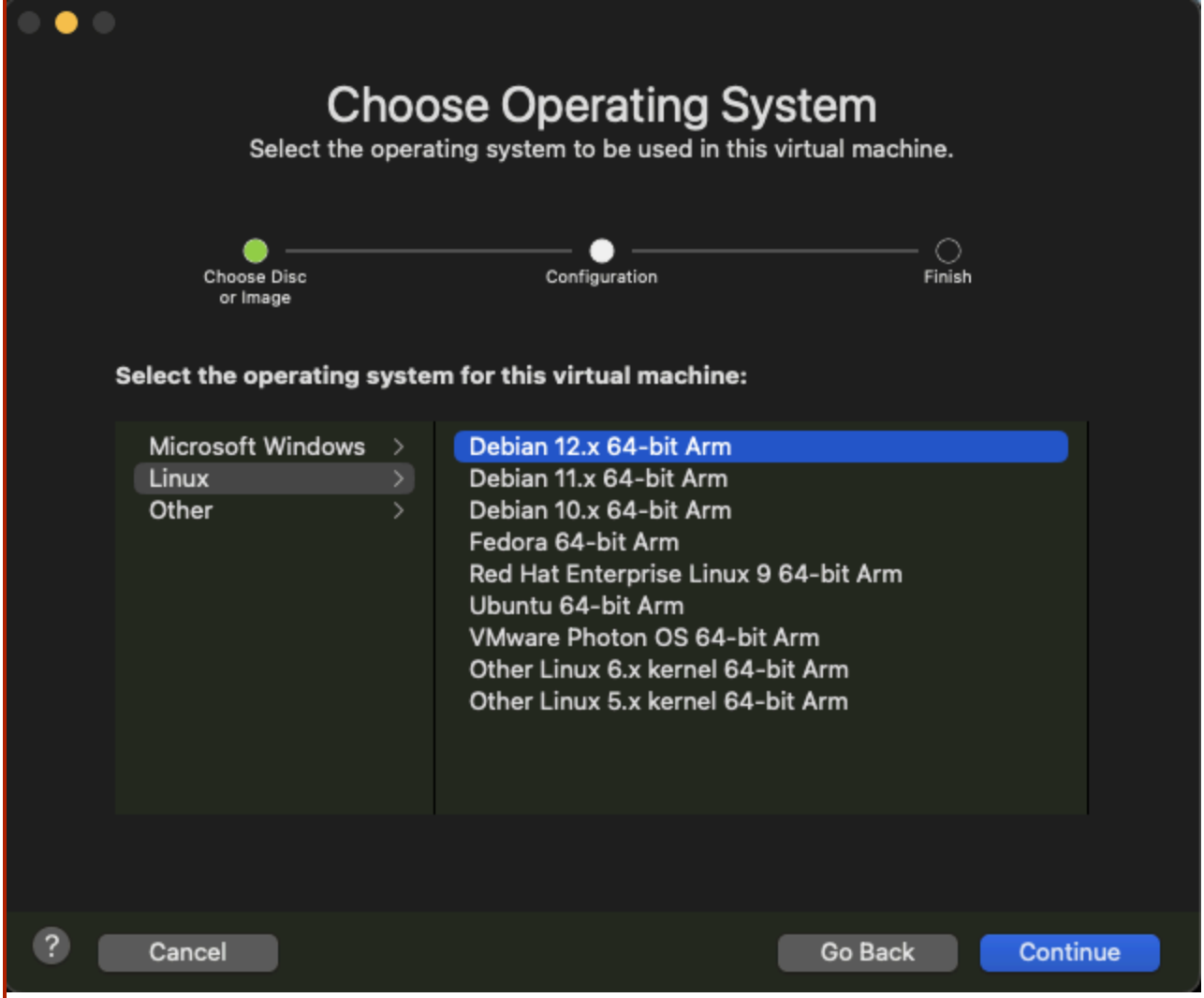

## VMware Fusion New Machine Wizard

After installing VMware Fusion 13, and opening the application for the first time, it forces the user to create a new machine. Once you've created your machine, if you would like to create another you will need to select "create new machine" from the options.

Open the directory in which the .iso was saved after downloading. Drag the freshly downloaded .iso to the window and begin the installation (Debian 12.x 64-bit Arm). We can also just simply click on "install from disk or image", or "use another disc, or disc image" option from the VMware Fusion application window.

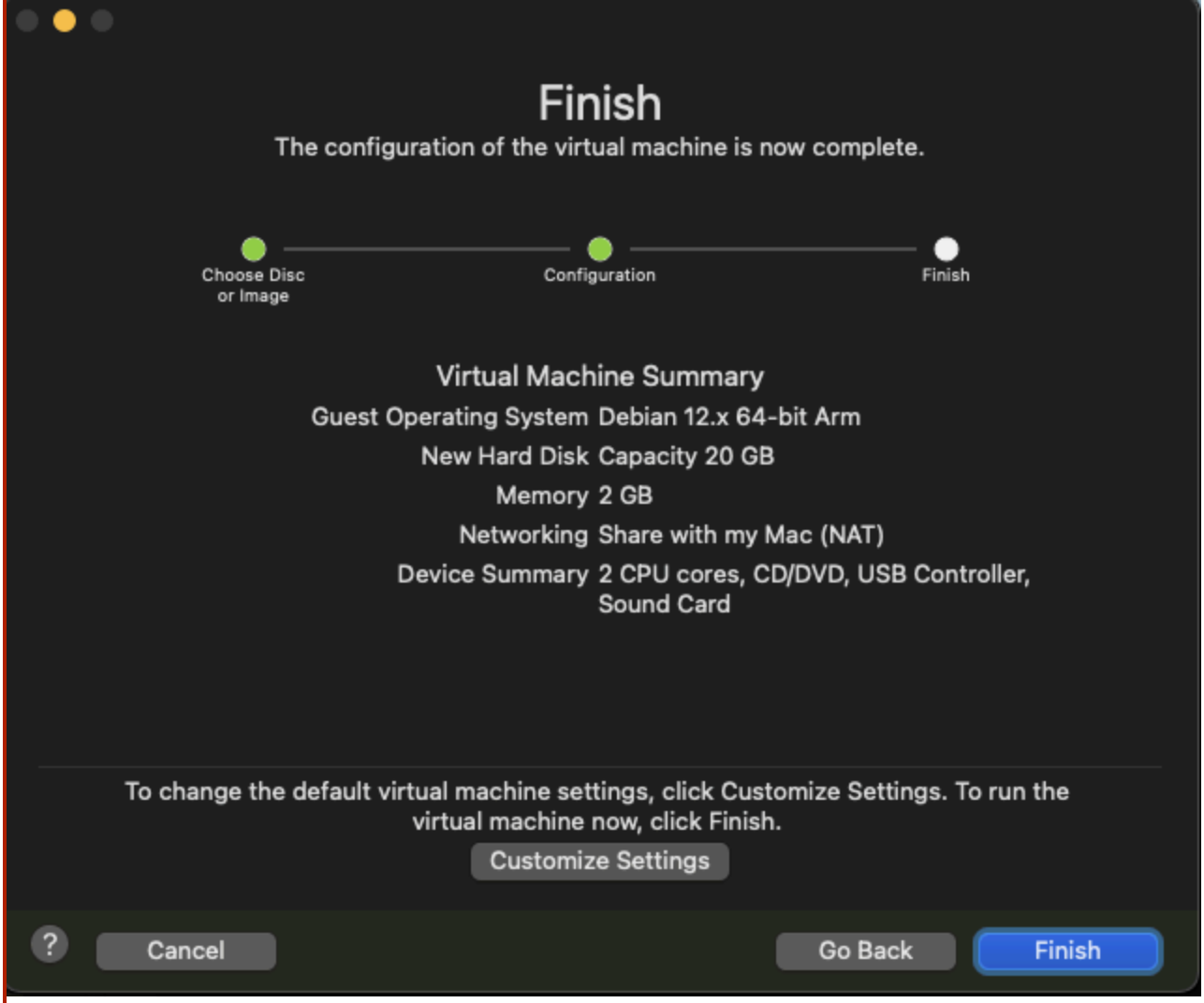

Select the Installation Method
Install from disc or image
Drag your ISO file here to start installing
Create a custom virtual machine
Get Windows from Microsoft
Cancel
Continue


Create a New Virtual Machine
This will guide you through installing Windows or another operating system in a virtual machine on your Mac.
Choose Disc or Image
Configuration
Finish
Choose an operating system installation disc or image:
kali-linux-2023.3-installer-arm64.iso
Show in Finder
Use another disc or disc image...
Cancel
Go Back
Continue




### Note

In the configuration section (not pictured), you can change the Hard Drive size to 80 GB is you have the HD space on your Apple Laptop. You should also be able to change the RAM size for the kali VM to 4GB, again, if you have the RAM to support it on your Apple Laptop.




After all this is done, we save, start up the VM, and then continue installing Kali Linux as we normally would for a bare metal install (see below).

# Installing Kali Linux

> **Note**
>
> For latest, see https://www.kali.org/docs/installation/hard-disk-install/

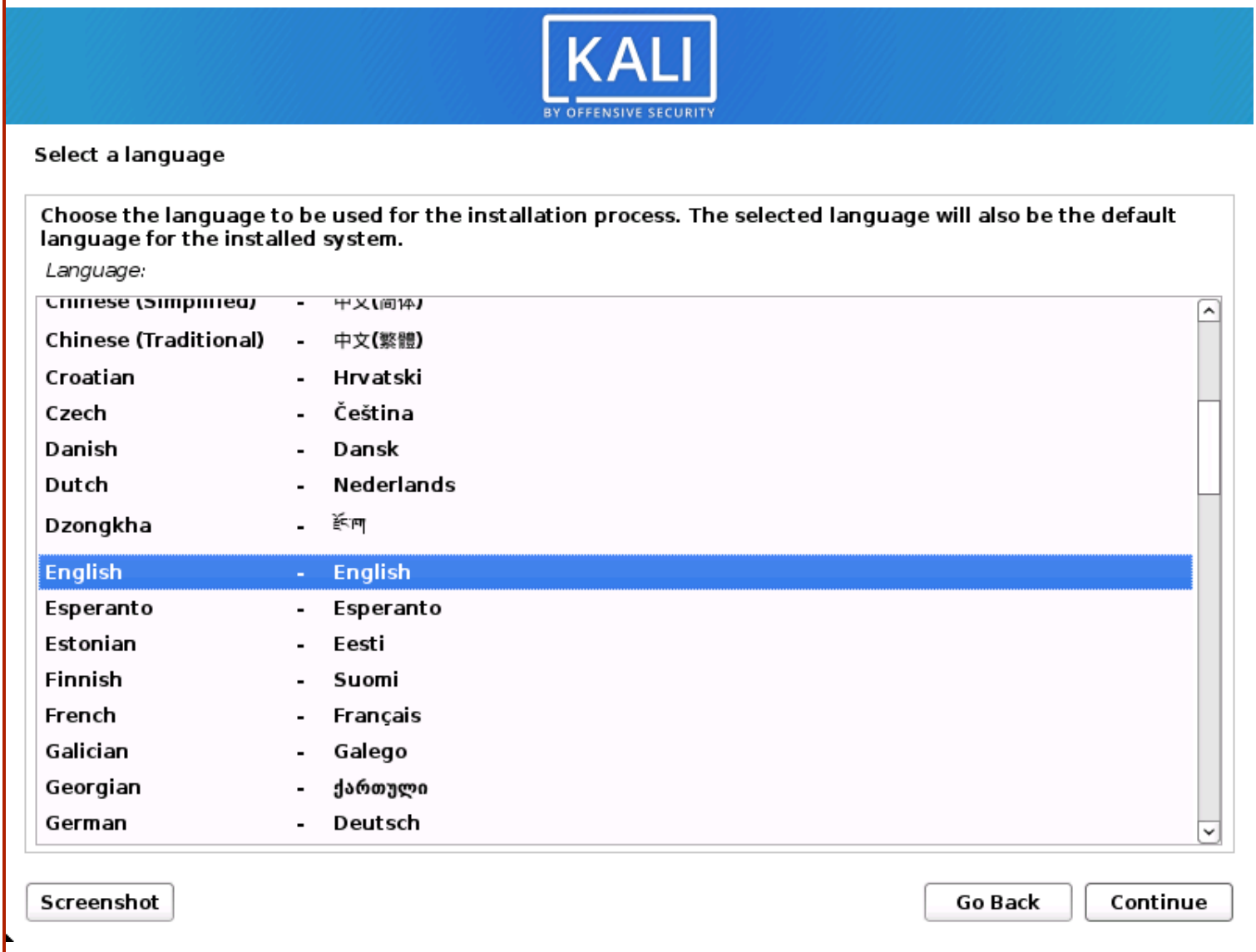
## Boot

1. To start your installation, boot with your chosen installation medium. You should be greeted with the Kali Linux Boot screen. Choose either **Graphical install** or **Install** (Text-Mode). In this example, we chose the Graphical install.

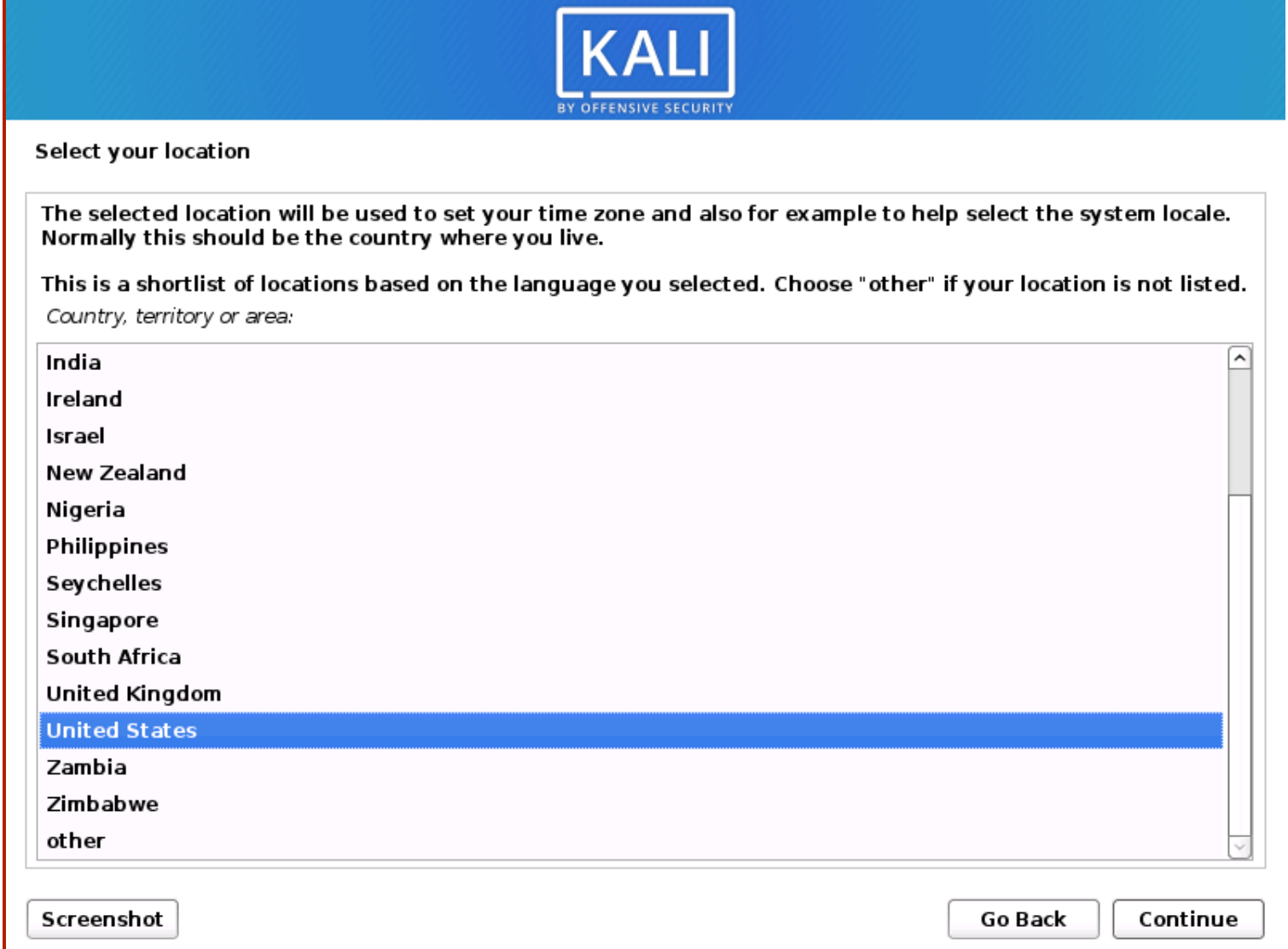

If you're using the **live** image instead, you will see another mode, **Live**, which is also the default boot option.

## Language

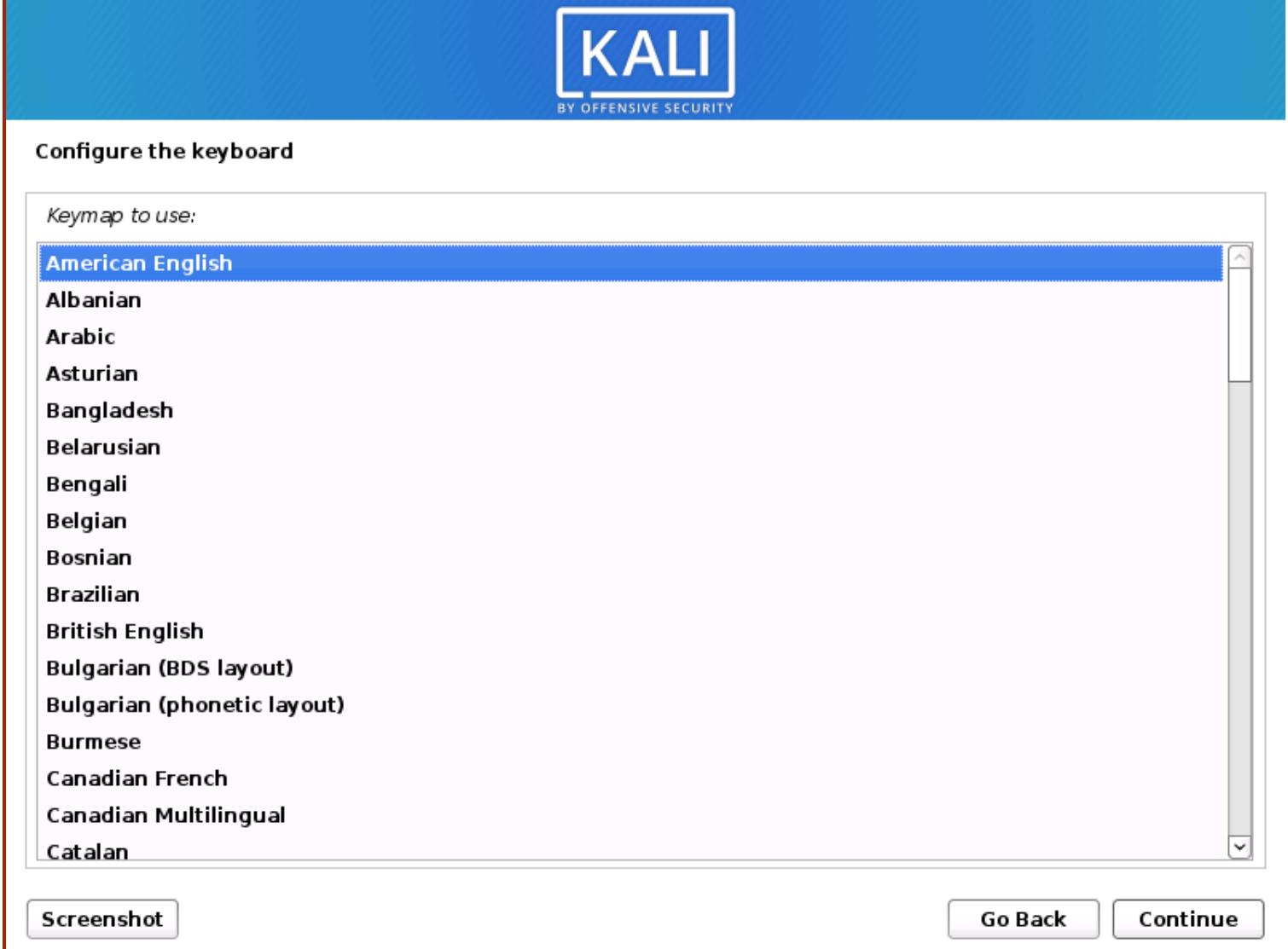
2. Select your preferred language. This will be used for both the setup process and once you are using Kali Linux.




3. Specify your geographic location.




4. Select your keyboard layout.

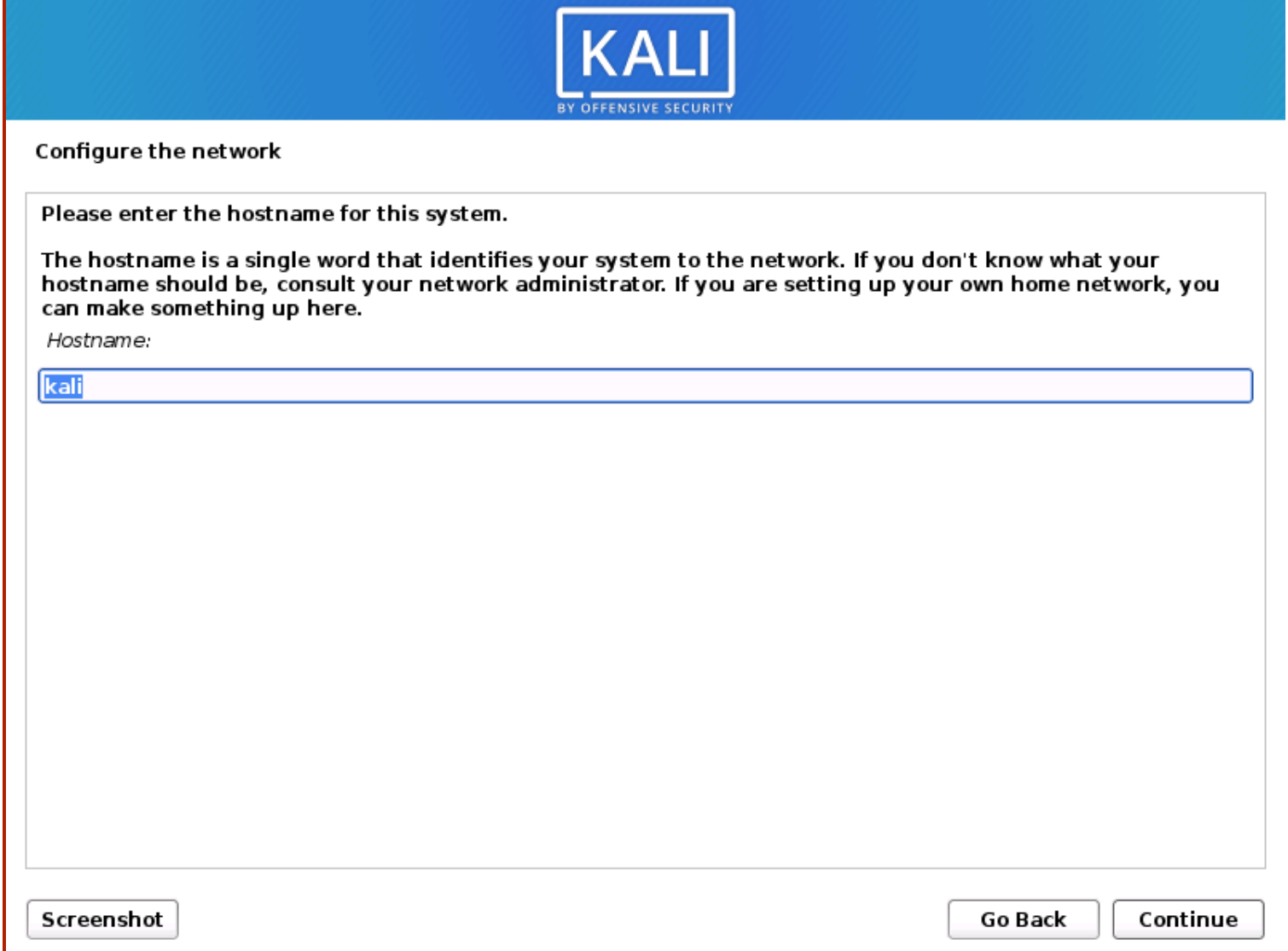



## Network

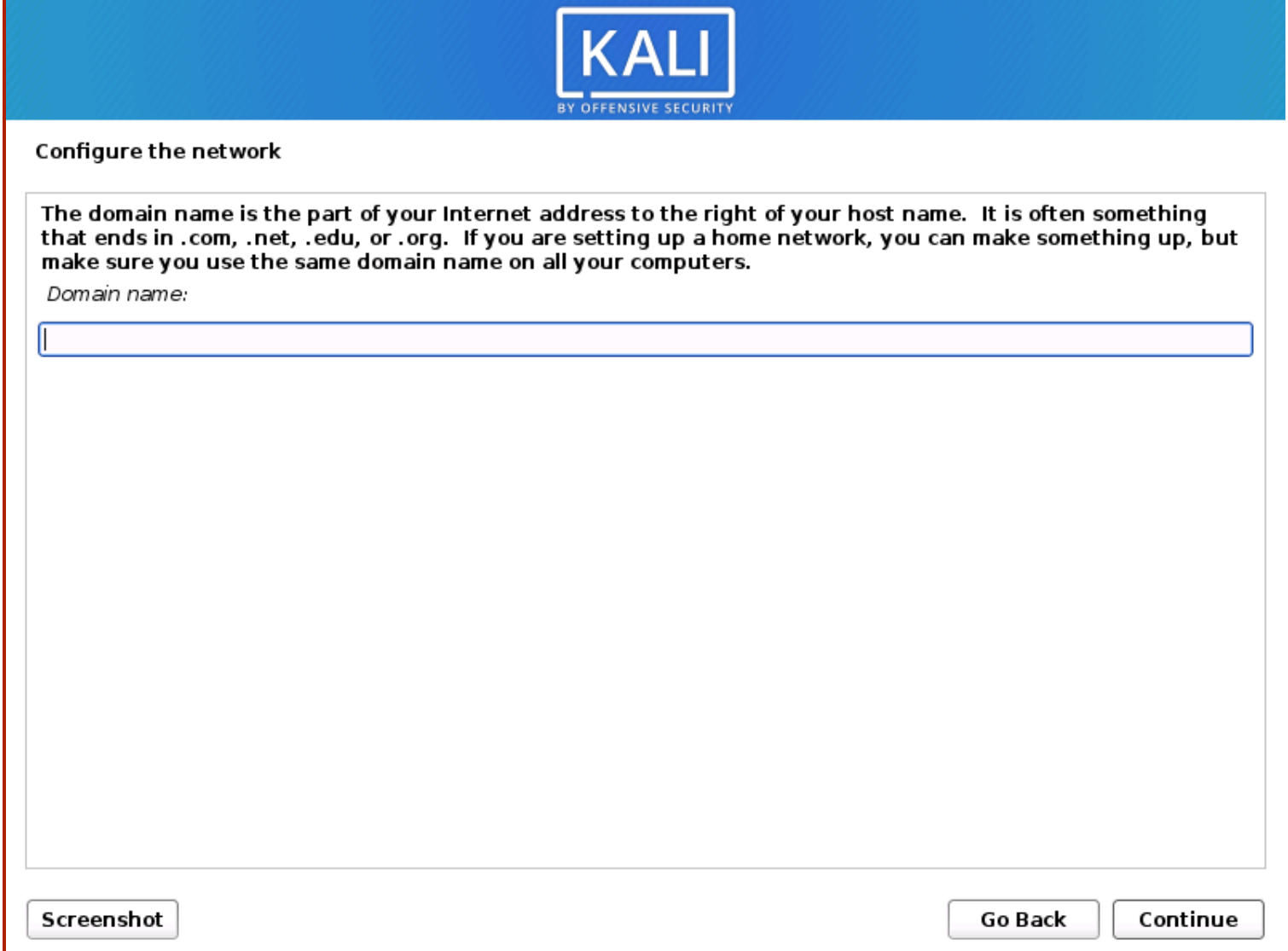
5. The setup will now probe your network interfaces, looks for a DHCP service, and then prompt you to enter a hostname for your system. In the example below, we've entered **kali** as our hostname.

If there is no network access with DHCP service detected, you may need to manually configure the network information or do not configure the network at this time.

- If there isn't a DHCP service running on the network, it will ask you to manually enter the network information after probing for network interfaces, or you can skip.
- If Kali Linux doesn't detect your NIC, you either need to include the drivers for it when prompted, or generate a custom Kali Linux ISO with them pre-included.
- If the setup detects multiple NICs, it may prompt you which one to use for the install.
- If the chosen NIC is 802.11 based, you will be asked for your wireless network information before being prompted for a hostname.




6. You may optionally provide a default domain name for this system to use (values may be pulled in from DHCP or if there is an existing operating systems pre-existing).




## User Accounts

7. Next, create the user account for the system (Full name, username and a strong 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:*

Kali

Screenshot | Go Back | Continue

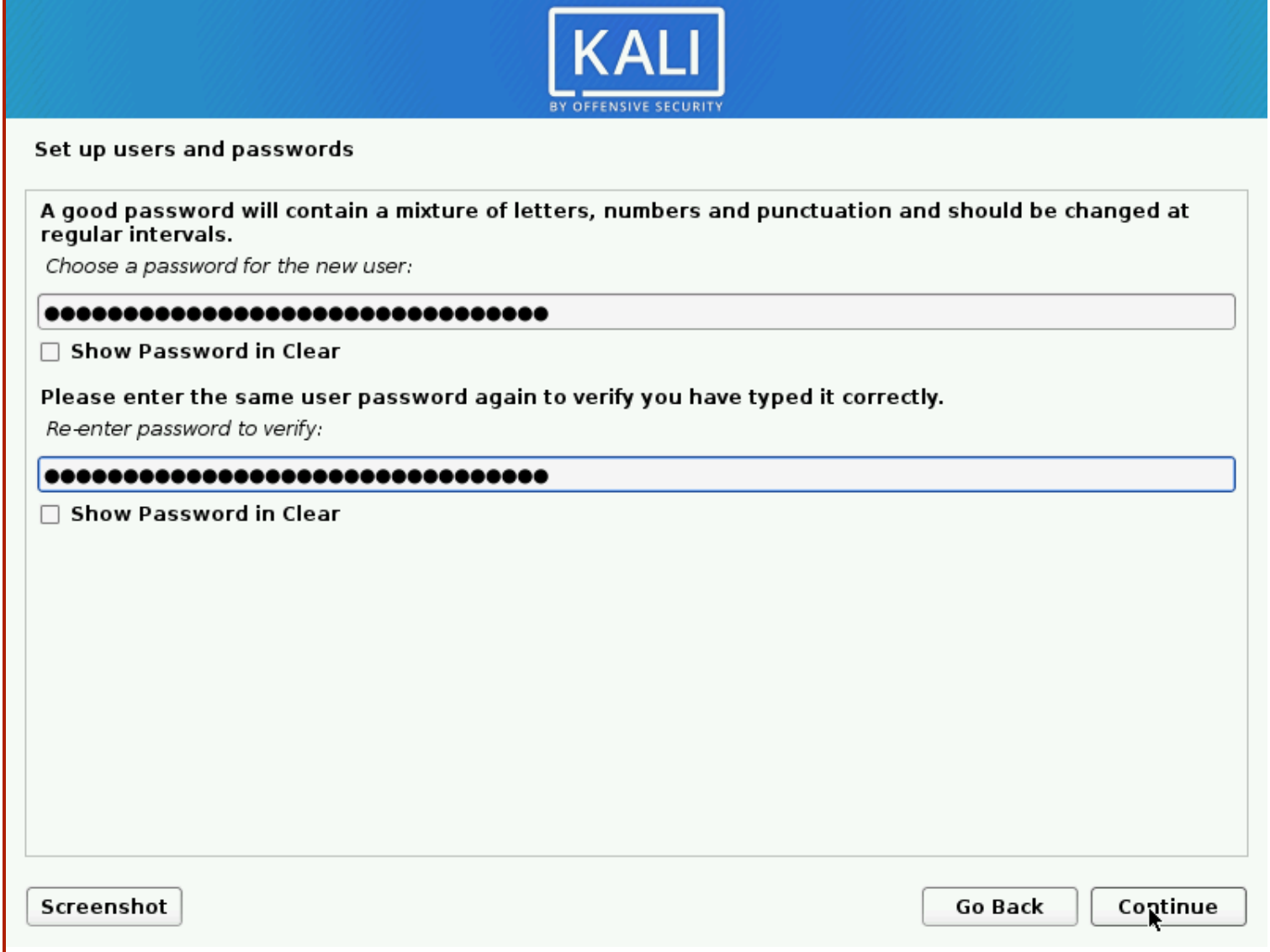

**Set up users and passwords**

**Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.**

*Username for your account:*

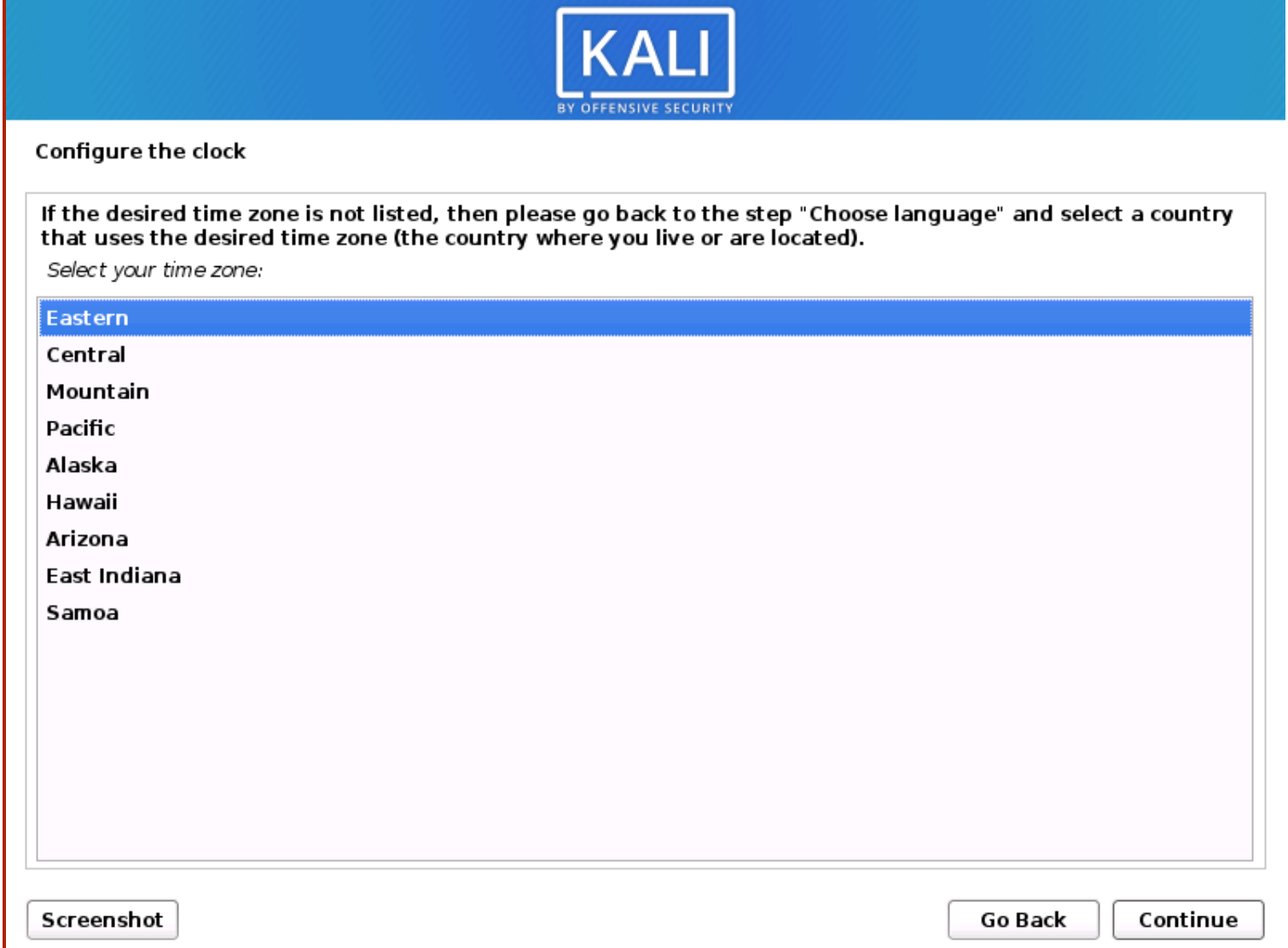
kali

Screenshot | Go Back | Continue




## Clock

8. Next, set your time zone.




## Disk

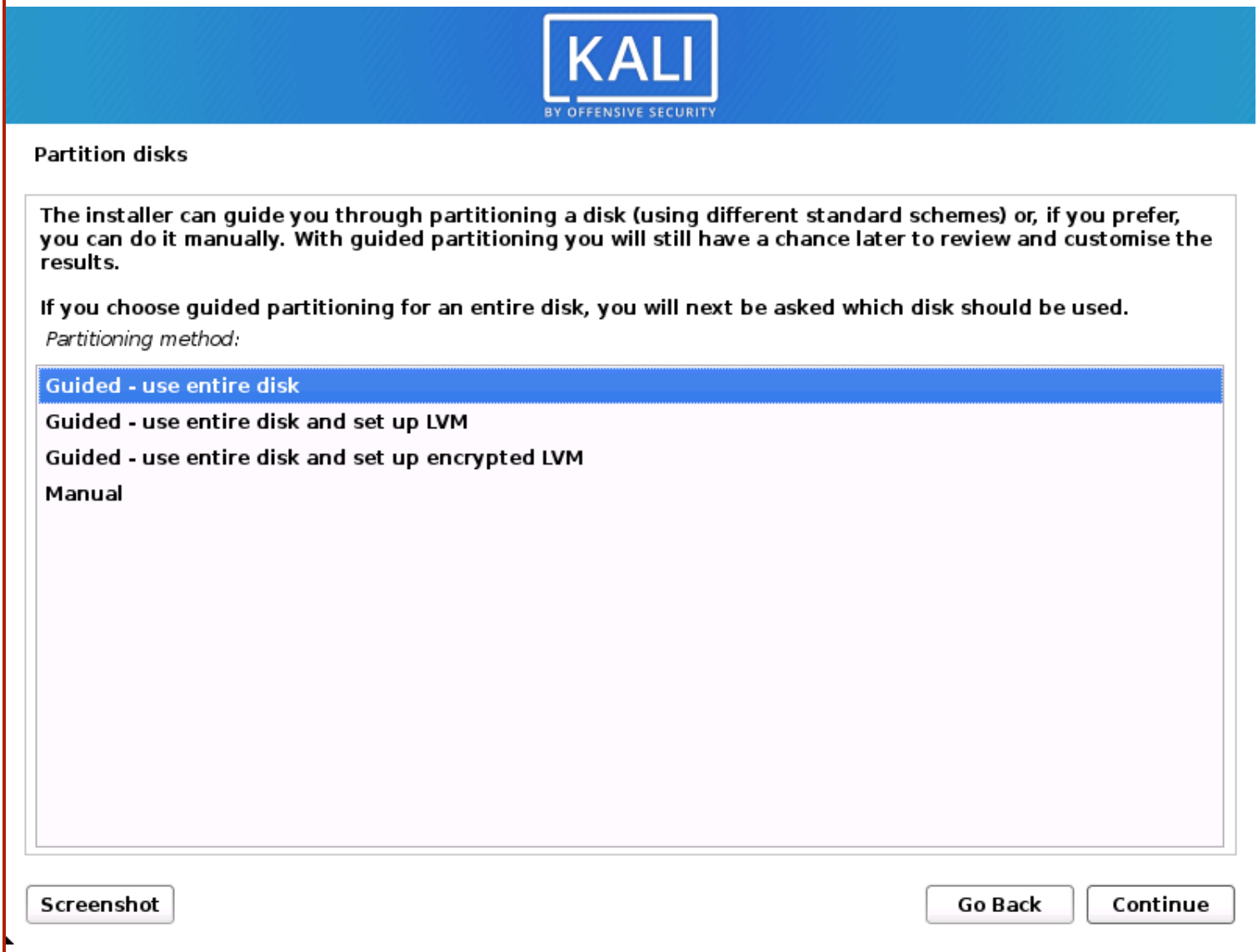
9. The installer will now probe your disks and offer you various choices, depending on the setup.

In our guide, we are using a clean disk, so we have four options to pick from. We will select **Guided - the entire disk**, as this is the single boot installation for Kali Linux, so we do not want any other operating systems installed, so we are happy to wipe the disk.

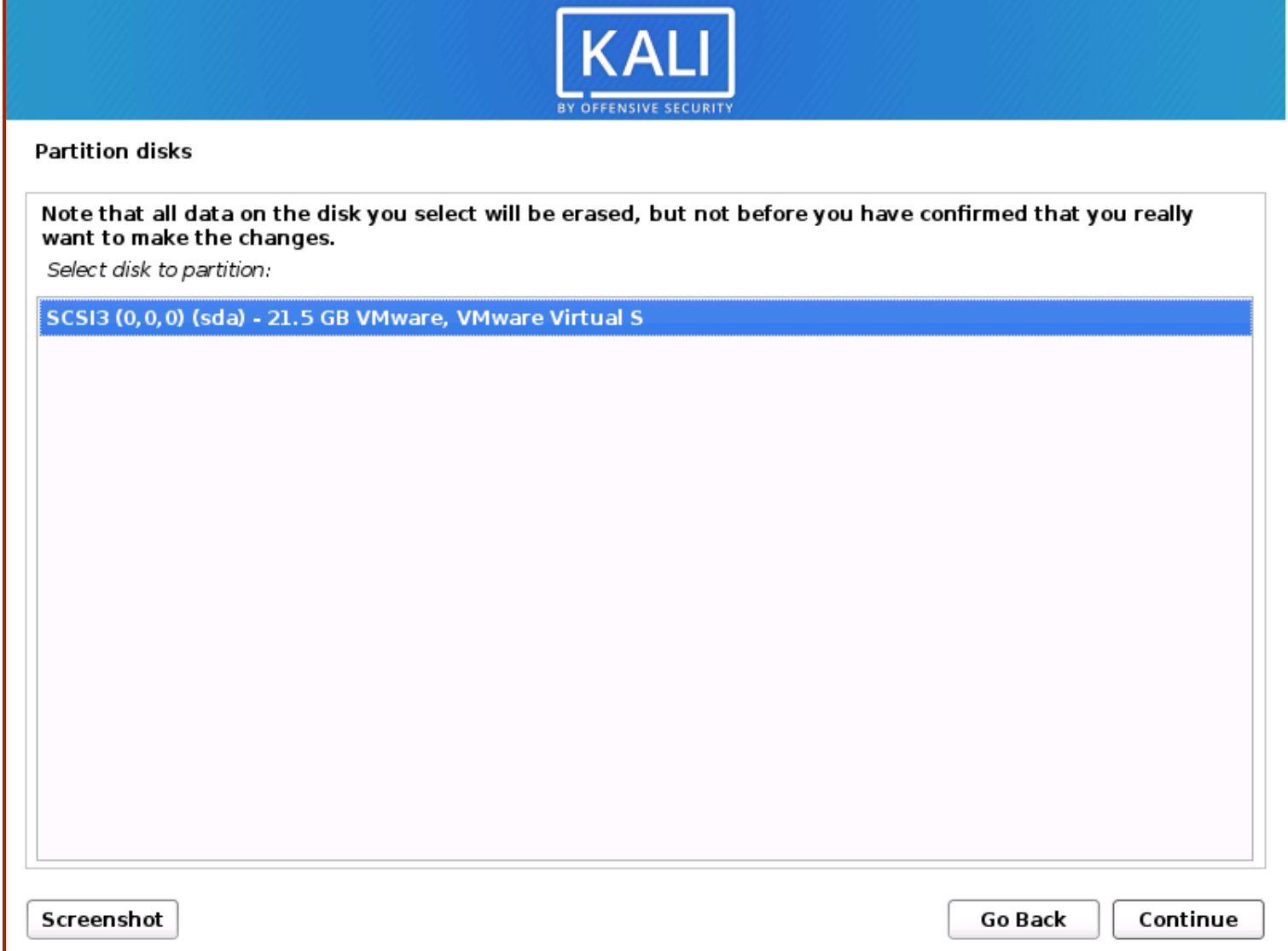
If there is an pre-existing data on the disk, you will have have an extra option *(Guided - use the largest continuous free space)* than the example below. This would instruct the setup not to alter any existing data, which is perfect for dual-booting into another operating system. As this is not the case in this example, it is not visible.

Experienced users can use the “Manual” partitioning method for more granular configuration options, which is covered more in our BTRFS guide.

If you want to encrypt Kali Linux, you can enable Full Disk Encryption (FDE), by selecting **Guided - used entire disk and setup encrypted LVM**. When selected, later on in the setup (not in this guide) prompt you to enter a password (twice). You will have to enter this password every time you start up Kali Linux.




10. Select the disk to be partitioned.




11. Depending on your needs, you can choose to keep all your files in a single partition - the default - or to have separate partitions for one or more of the top-level directories.

If you're not sure which you want, you want "**All files in one partition**".


Partition disks

Selected for partitioning:

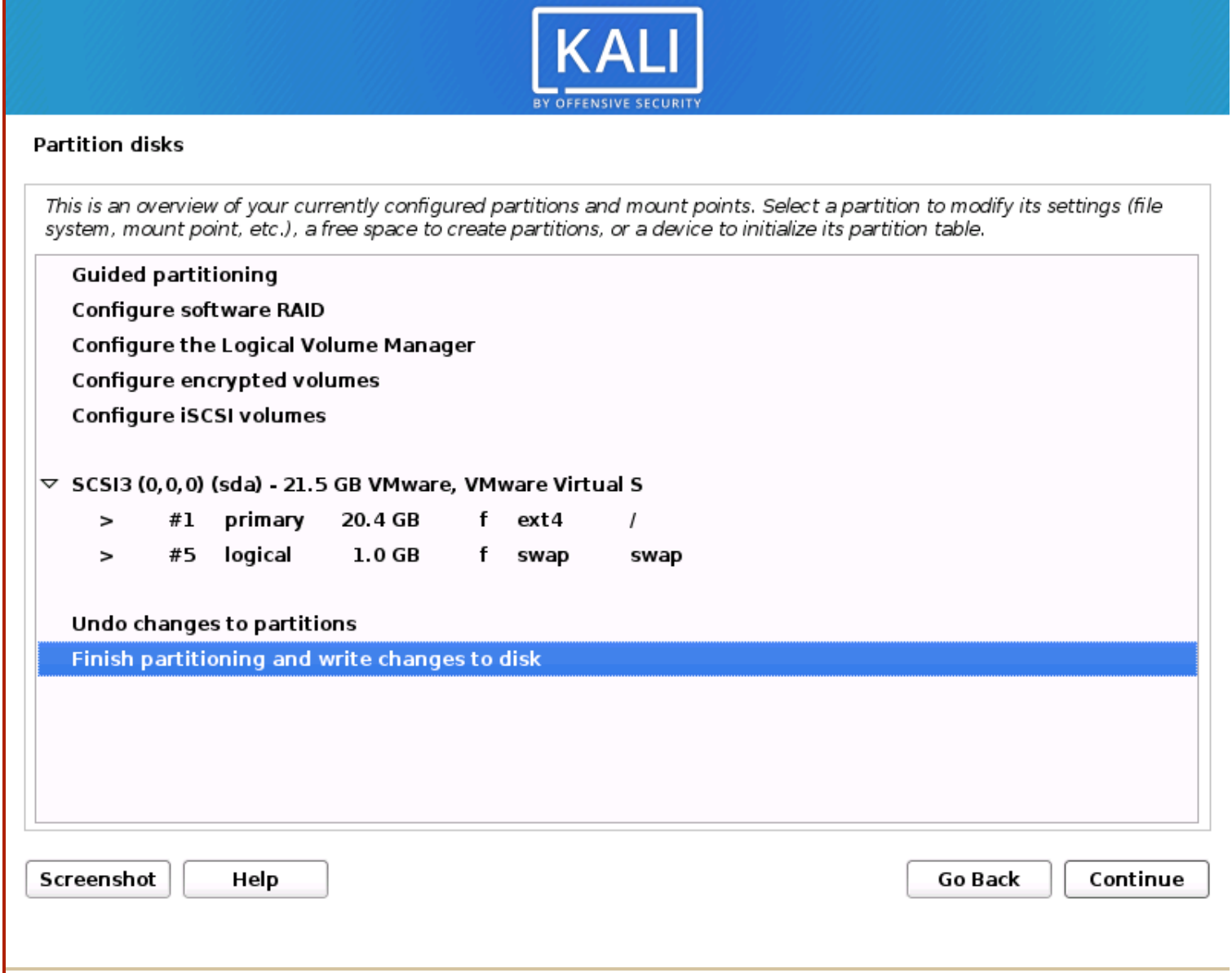
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB

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

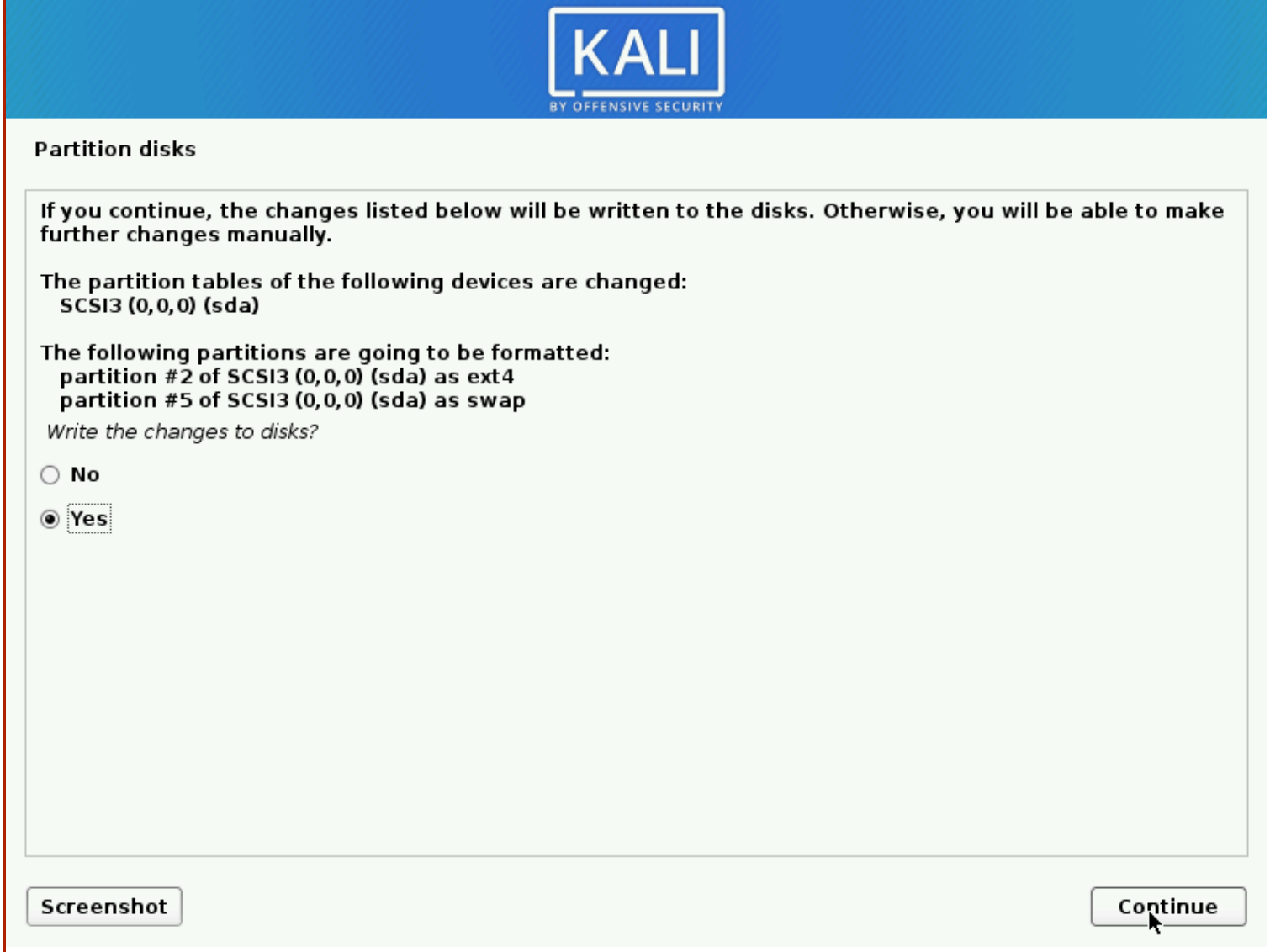
*Partitioning scheme:*

- All files in one partition (recommended for new users)
- Separate /home partition
- Separate /home, /var, and /tmp partitions

Screenshot | Go Back | Continue




12. Next, you'll have one last chance to review your disk configuration before the installer makes irreversible changes. After you click *Continue*, the installer will go to work and you'll have an almost finished installation.




## Encrypted LVM

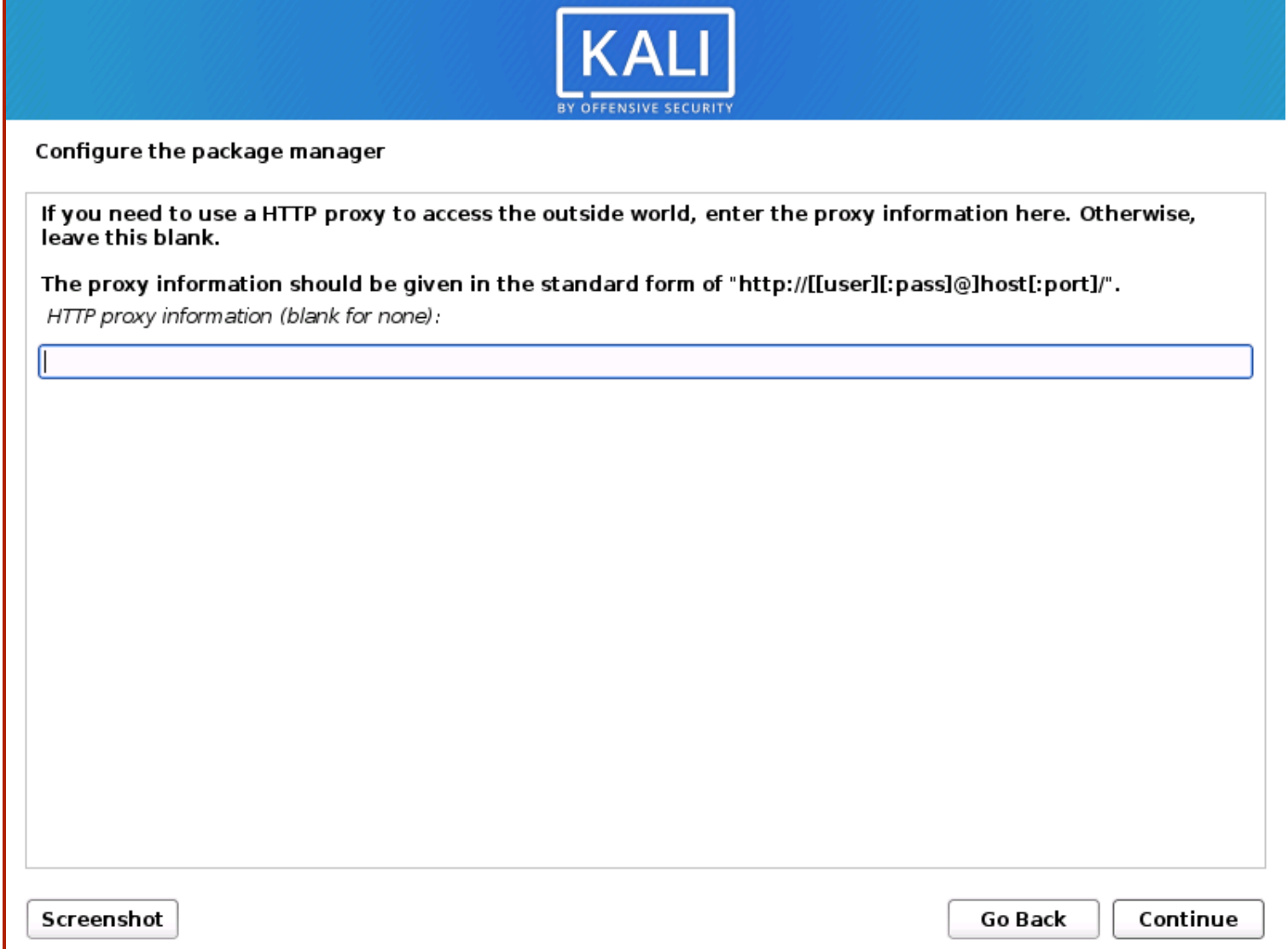
If enabled in the previous step, Kali Linux will now start to perform a secure wipe of the hard disk, before asking you for a LVM password.

Please be sure a strong password is used, or else you will be prompted with a weak passphrase warning.

This wipe may take “a while” (hours) depending on the size and speed of the drive.
If you wish to risk it, you can skip it.

## Proxy Information

13. Kali Linux uses a central repository to distribute applications. You’ll need to enter any appropriate proxy information as needed.



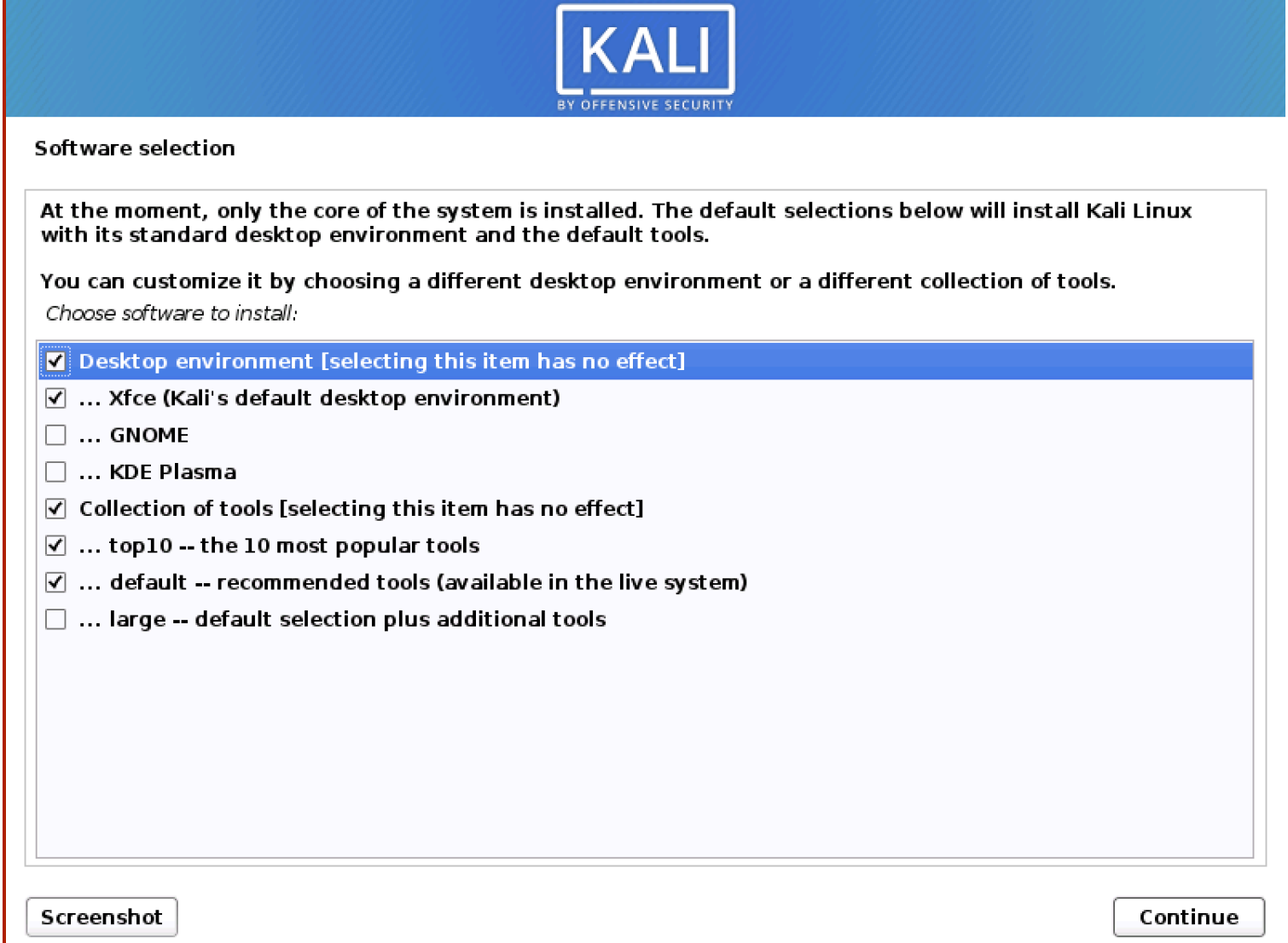

## Metapackages

If network access was not setup, you will want to **continue with setup** when prompt.

If you are using the **Live** image, you will not have the following stage.

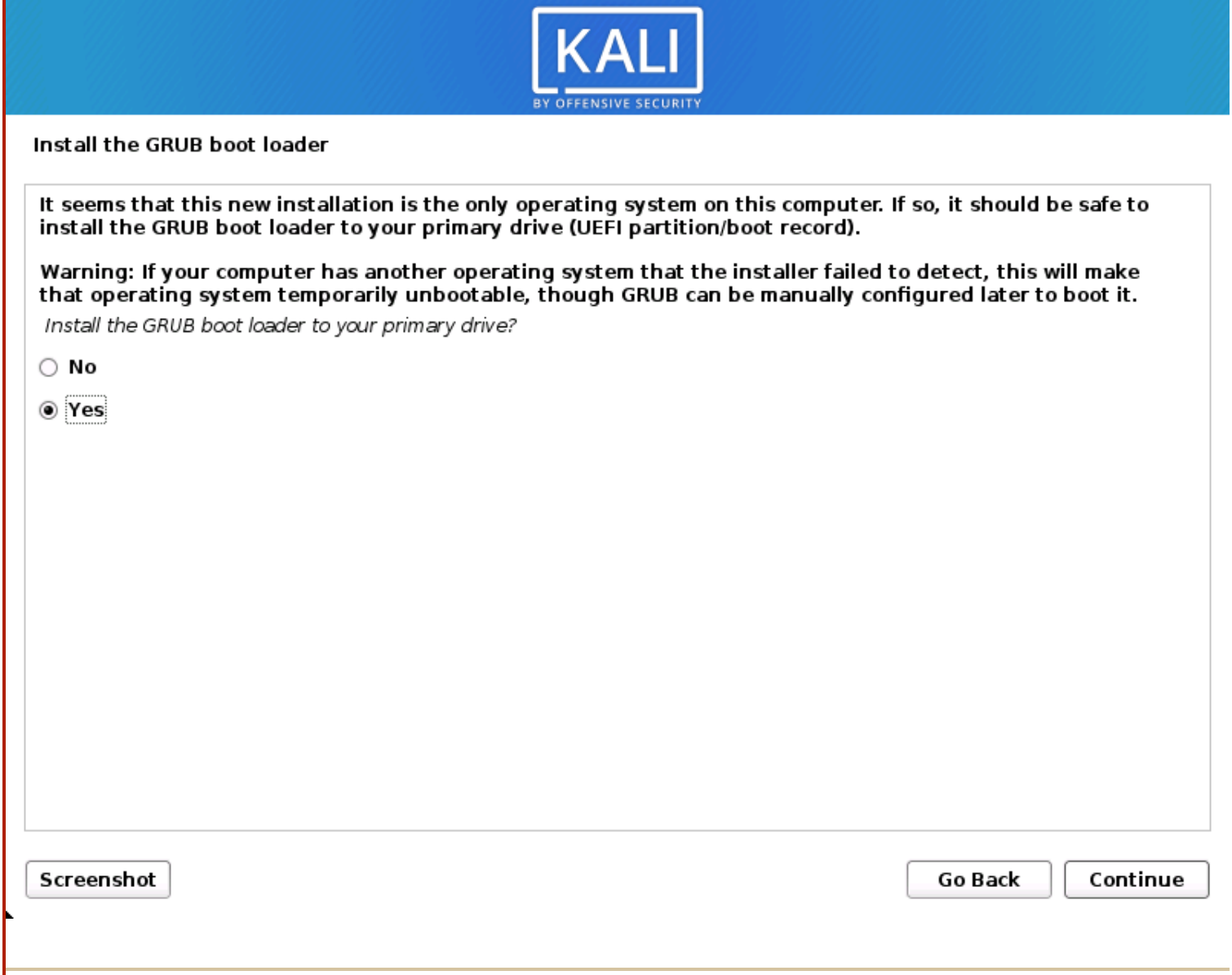
14. Next you can select which metapackages you would like to install. The default selections will install a standard Kali Linux system and you don't really have to change anything here.

Please refer to this guide if you prefer to change the default selections.

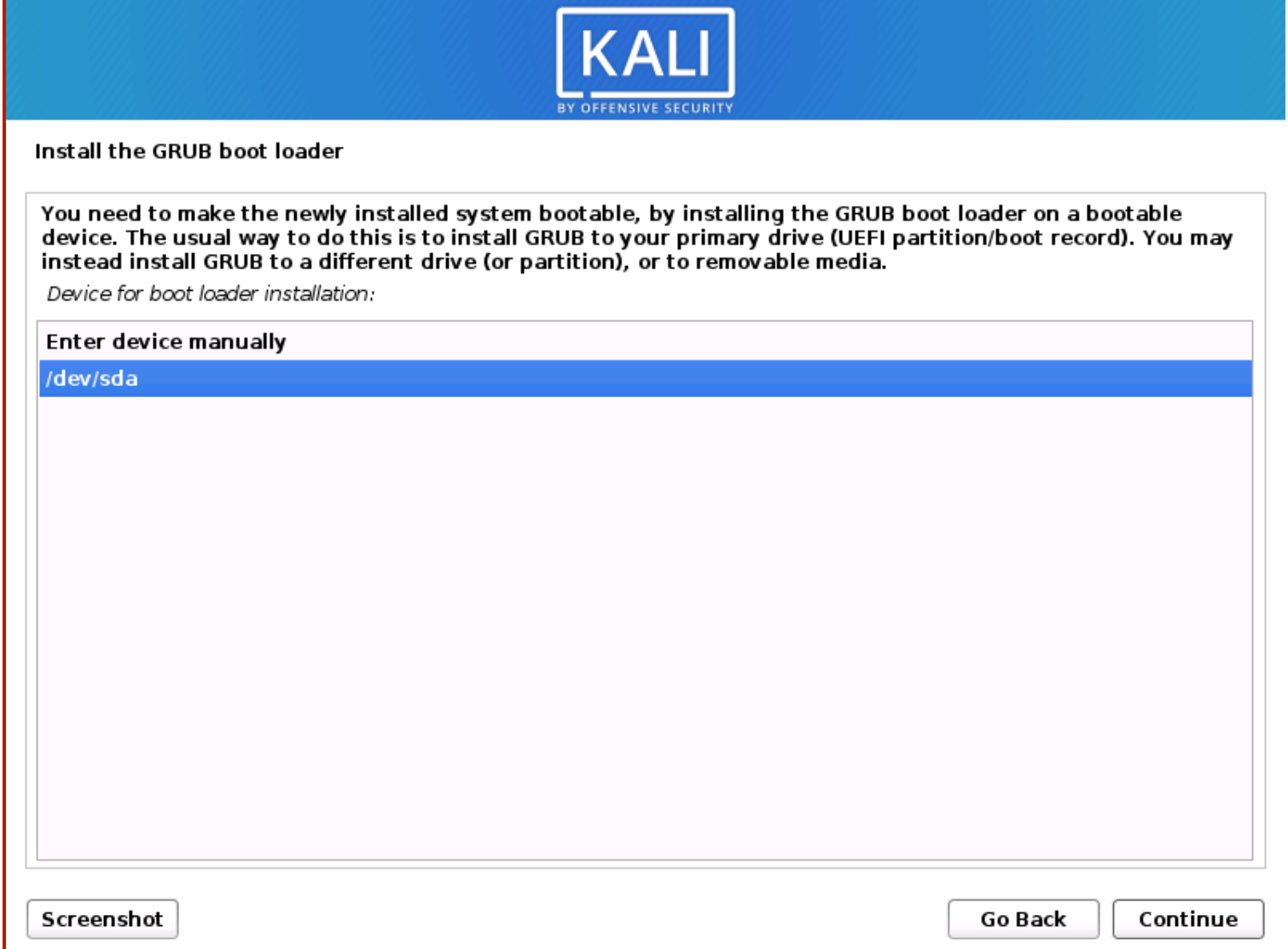



## Boot Information

15. Next confirm to install the GRUB boot loader.

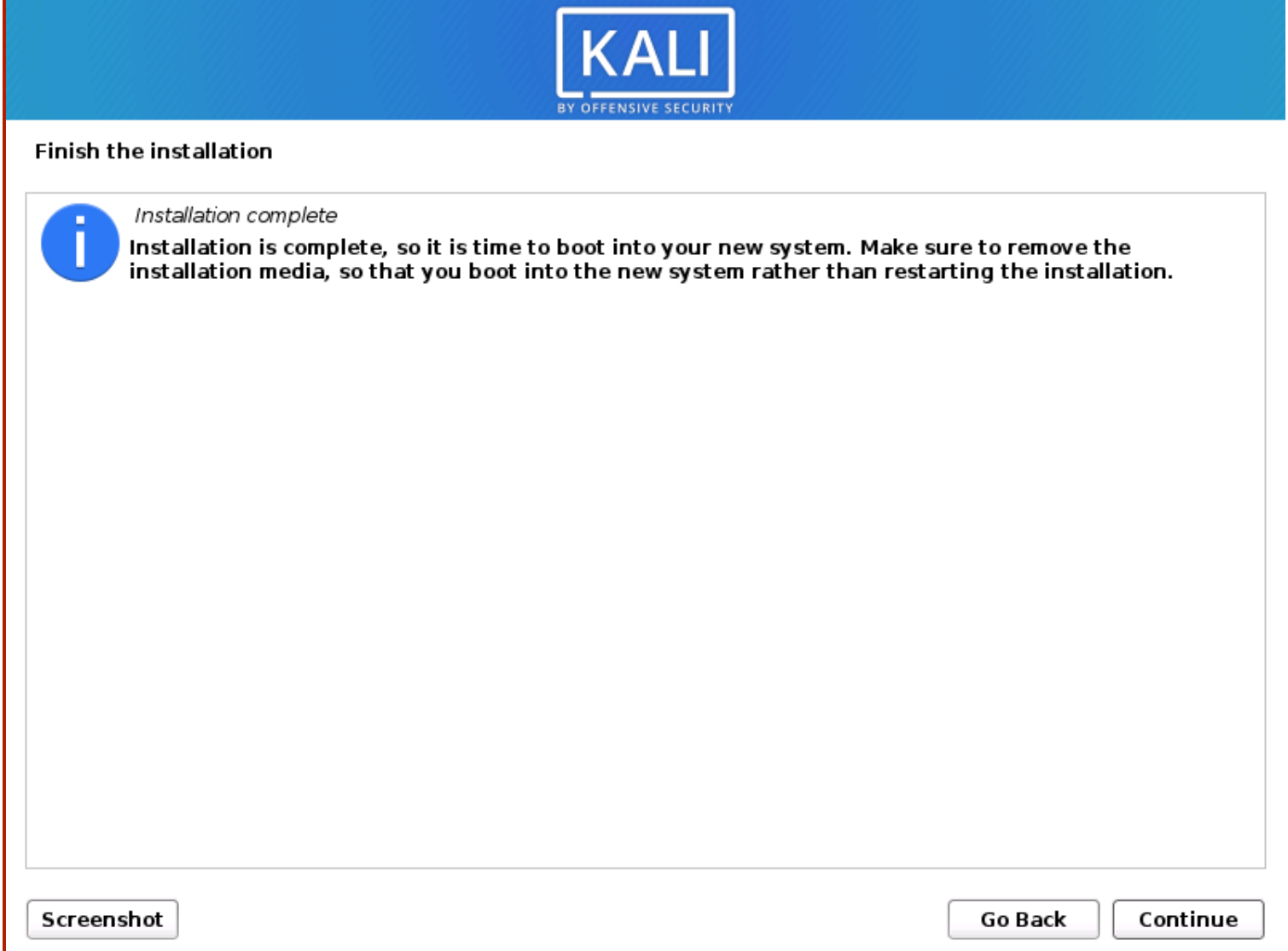



16. Select the hard drive to install the GRUB bootloader in (**it does not by default select any drive**).




## Reboot

17. Finally, click Continue to reboot into your new Kali Linux installation.

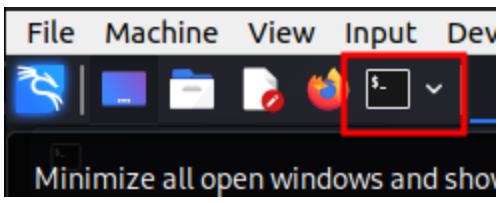



## Post Installation

Now that you've completed installing Kali Linux, it's time to customize your system, but before the next steps, take a snapshot of the VM before going further.

## Step 3 - Run the setup script:

- Start the new Kali VM
- Log into fresh Kali VM using the creds you set up from above:
- Open the Terminal
  - The button can be found in the upper left of the desktop:




- The following commands will need to be run from within the terminal:

> ⚠ **Warning**
> If you copy from the PDF, you may need to fix the lines in a text file first before using it in the terminal (it may chop it up in the copy). Copy it, then paste into you're favorite text editor and then re-copy it.

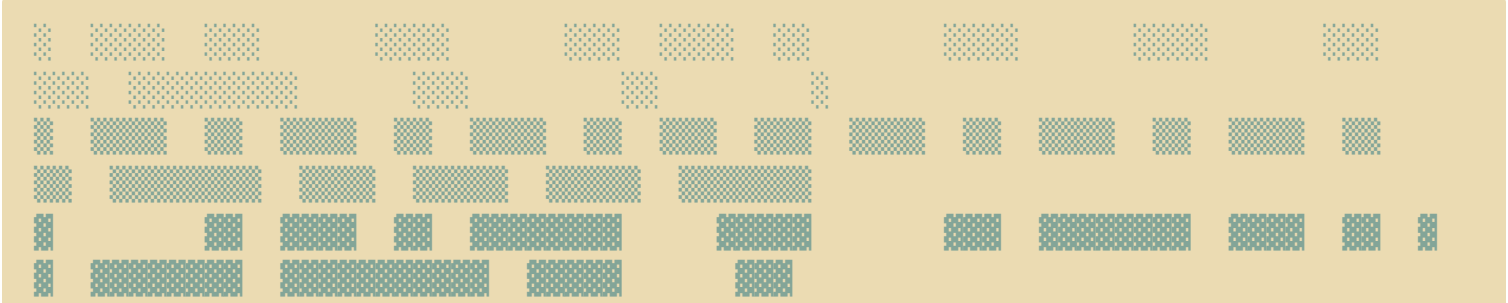
`mkdir Projects && cd Projects && git clone https://github.com/bkarnes/hack3rcon_ctf.git && cd hack3rcon_ctf && chmod u+x setup_vm.sh && ./setup_vm.sh`

### Explanation of the above commands:

- We make a Projects directory in kali's home directory:
  `mkdir Projects`
- We then change into the Projects directory
  `cd Projects`
- We clone my Repo:
  `git clone https://github.com/bkarnes/hack3rcon_ctf.git`
- We then change into the LinuxAdminClass directory that is created:
  `cd hack3rcon_ctf`
- We make the setup_vm.sh script executable:
  `chmod u+x setup_vm.sh`
- We then run the script:
  `./setup_vm.sh`

## Running the Script:

> ⚠ **Warning**
>
> The script has only been tested on Kali, but may not work on ParrotOS.
> Also, use the user creds you set above instead of the kali creds from the VM
> To restart the script after the first step, run the following:
> `./Projects/hack3rcon_ctf/setup_vm.sh`



```
Today is: Sat May 24 02:08:09 PM EDT 2025
What can I do for you today?

1) Setup CLI logging and default directories.  Will require a reboot.
2) Update VM.  Will reboot after update.
3) Install Docker.  Will reboot after install.
4) Install netbird client.  Will reboot after install.
5) Install Project Discovery Tools.(Optional)  Will reboot after install.

(Q)uit
```

- Now, perform the following actions in the following order (reboot as needed):

> **Note**
> The VM will reboot after each step

1. Setup CLI logging.
   You will need to put in kali's password twice
2. Update VM.
   This step is optional if you've already updated your VM this before running the script or can be done after other steps are completed.

   This could take a long time depending on your Internet speed and HD. Plus, you may need to watch it a bit as you will need to put in kali's password a couple of times and maybe answer a question or two.
3. Install Docker.
4. Skip the netbird client step as you will set it up below (due to the Arm architecture).
   - You will use a netbird setup key below
5. Install the Project Discovery tools if you would like (not required for the CTF)

> **Warning**
> You will need to enter the user's creds to reboot after this step is finished.

- Quit out of the script and run the following to install the netbird agent:
  `curl -fsSL https://pkgs.netbird.io/install.sh | sh`

## Step 4 - Test the setup:

- Reboot it one last time and run the following tests:
  - [ ] Ensure that the kali user has the BASH shell loaded:

```
┌──(kali㉿kali)-[~]
└─$ echo $SHELL
/bin/bash
```

    - If you don't see **/bin/bash** like above, then run the following command:
      `chsh -s /bin/bash`
    - Reboot the VM and rerun the echo command from above to ensure is says **/bin/bash**.
  - [ ] Check to make sure Netbird installed properly:

```
┌──(kali㉿kali)-[~]
└─$ netbird version
0.29.1

Your version may be newer.
```

  - [ ] Make sure netbird is not connected to any network and then connect it to the CTF network:

```
┌──(kali㉿kali)-[~]
└─$ netbird down
Disconnected

┌──(kali㉿kali)-[~]
└─$ sudo netbird up --setup-key 61321F92-BF18-4D44-A6EB-9E72C84D9ABD
[sudo] password for kali:
Connected
```

## Step 5 - Playing the CTF:

- To play the CTF this year, you will work from your VM and connect to the servers in the CTF Network using Netbird. The scoreboard will be available the day of the event so teams can sign up on Friday, Oct. 24th, starting at 9 am.

## Appendix

# Doing Check Sums on downloaded files:

After downloading the following files, you will need to do a check sum on the file to ensure it is exactly as the one on the server. To do that, select one of the following to run the checksums:

## Check Sums (Windows):

- File Checksum & Integrity Check on Windows 10 - File Security [Hash SHA-1/256/384/512/MD5] - https://www.youtube.com/watch?v=UrHhsF1q3rU
- Verifying a SHA Checksum on Windows 10 - https://www.youtube.com/watch?v=6Xpmku3kwjo
- Use the following command for checking the sums on windows: `certutil -hashfile "filename.zip" sha256`

## Check Sums (MacOS):

Verifying a SHA Checksum on a Mac is the same as the Linux Commands below due to their similar nature.

## Check Sums (Linux):

```
echo "sha256 hash line" | shasum -a 256 --check

Example:
echo "6a9faee5c0a2573598704a09864d6072a0685269707c186dfc8ebde4551ee5c3
VMware-Fusion-13.6.1-24319021_universal.dmg" | shasum -a 256 --check

Result:
VMware-Fusion-13.6.1-24319021_universal.dmg: OK
```

Alternatives ways to do it on the CommandLine:

```
shasum -a 256 SecureWV-PlayerVM.7z

sha256sum VMware-Fusion-13.6.1-24319021_universal.dmg
6a9faee5c0a2573598704a09864d6072a0685269707c186dfc8ebde4551ee5c3  VMware-
Fusion-13.6.1-24319021_universal.dmg

Then you will need to compare with the number from the website.
```