Setup The Attacker Machine

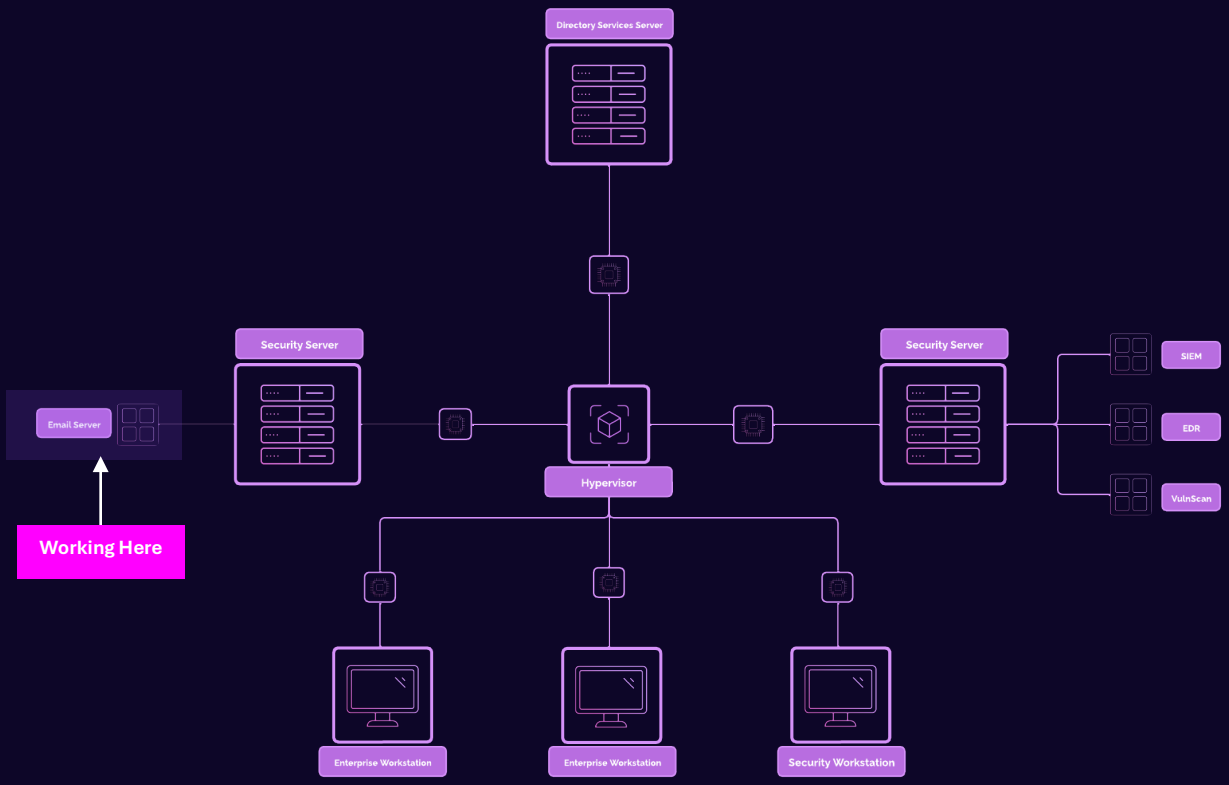
>prøjectsecurity_

Table of Contents

Prerequisites

1. Virtual Box Installed.
2. Virtual Machine with Kali Linux ISO has been configured and provisioned (the ISO should be attached to the new VM).

Network Topology



Kali Linux Overview

What is Kali Linux?

Kali Linux is a specialized Linux distribution tailored for cybersecurity professionals and ethical hackers. Developed by Offensive Security, it is a Debian-based operating system preloaded with tools designed for penetration testing, ethical hacking, and digital forensics. Kali Linux is widely used for assessing system vulnerabilities, testing network security, and investigating cyber incidents.

Kali comes with a suite of security tools to assist in the operations.

How is Kali Linux Used?

Kali Linux serves multiple purposes in the cybersecurity field, including:

1. **Penetration Testing**:
   Professionals use Kali Linux to simulate real-world cyberattacks and identify vulnerabilities in systems, networks, and applications. Tools like Metasploit and Burp Suite are often employed in these scenarios.
2. **Vulnerability Assessment**:
   It provides tools to scan and identify weaknesses in infrastructure, ensuring they are addressed before exploitation.
3. **Cybersecurity Training:**
   Kali Linux is widely used in cybersecurity training programs, competitions, and certifications.

Security Implications

Leveraging an operating system like Kali Linux carries certain benefits and risks.

Benefits

- Can be used by trained professionals to help understand their organizational security controls and identify vulnerabilities before actors can exploit them.
- Offers a platform to safely practice offense security techniques in controlled environments.
- Tools are aggregated in one centralized ecosystem.

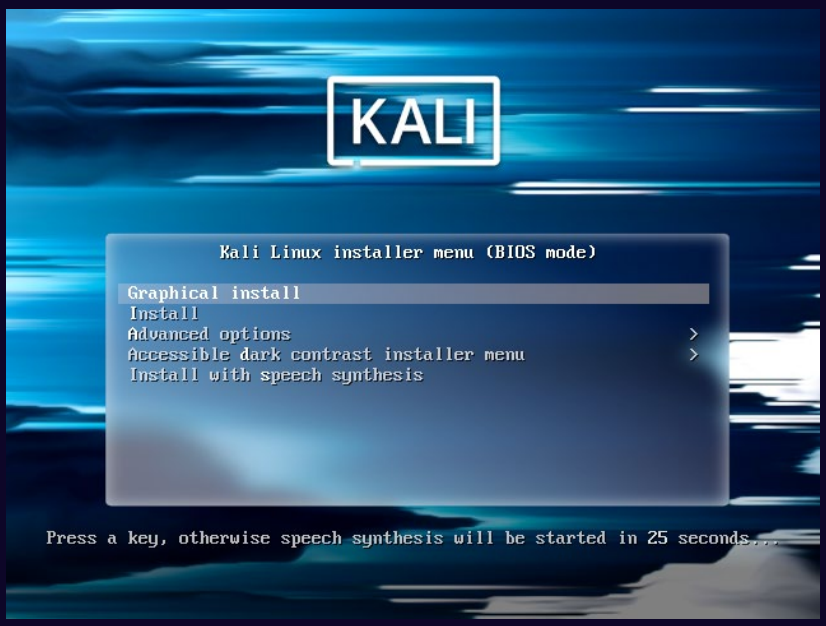
Risks

- This tool can also be used maliciously by attackers if accessed by unauthorized individuals.
- Kali Linux is not meant to be a production environment without isolation. Be careful.

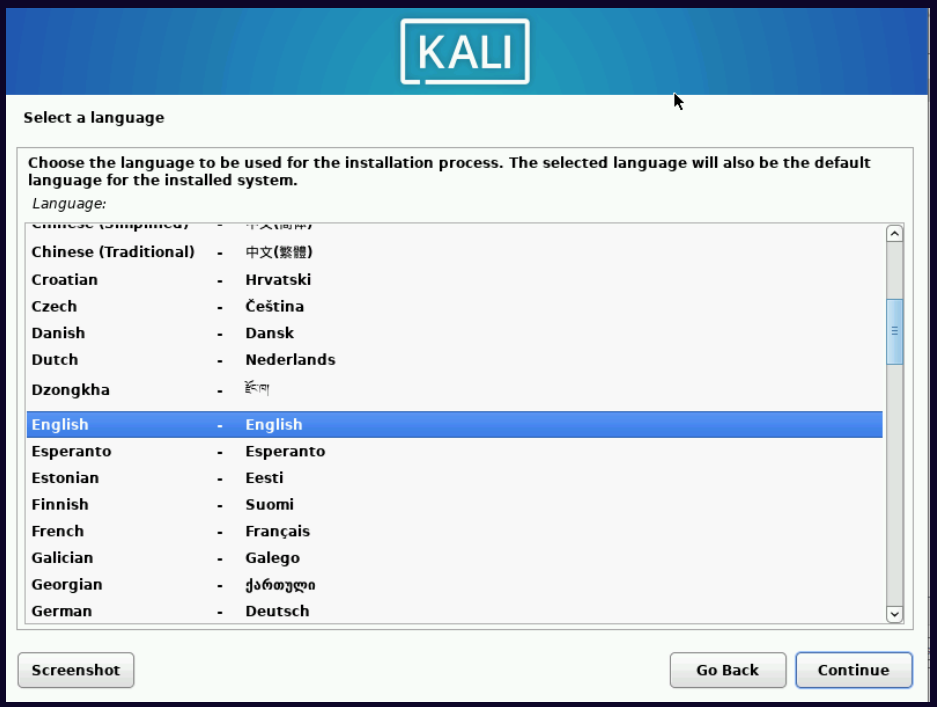
Configure Kali Linux

Step 1

Choose the default “Graphical install”.

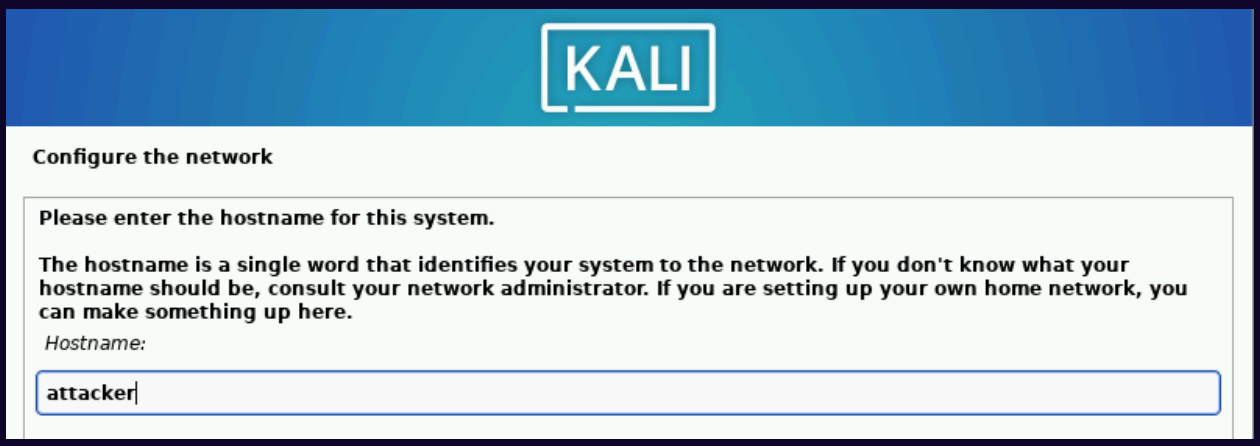


Choose Language → “Continue”.

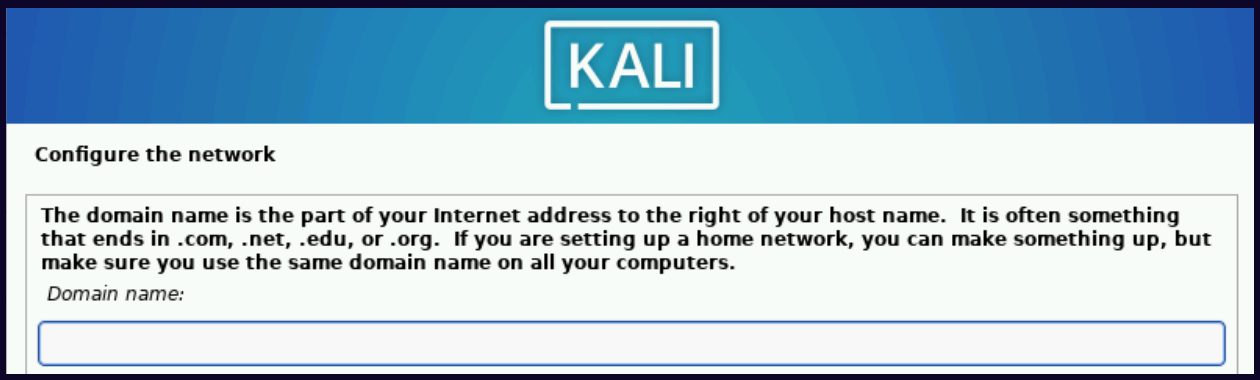


Choose the Country and Keyboard layout.

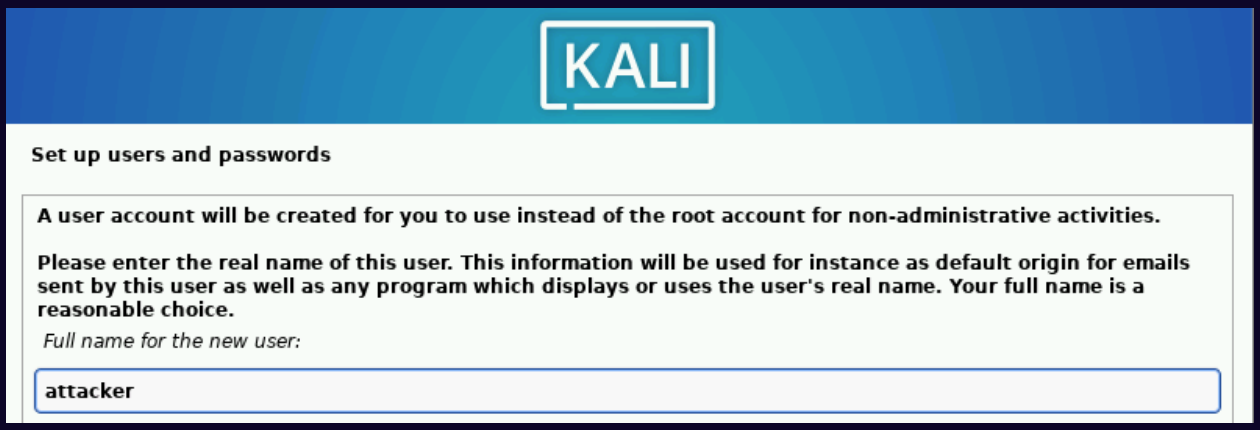
Change the hostname from Kali to attacker → “Continue”.

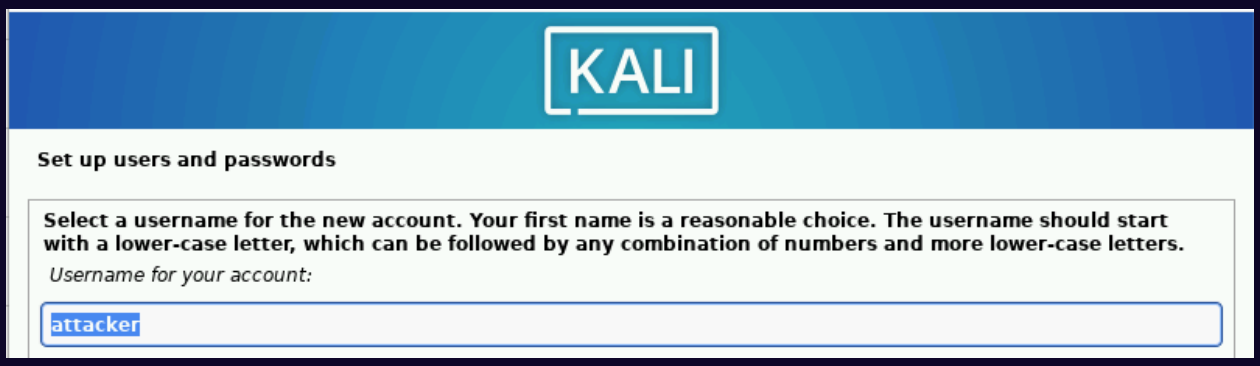


Leave the domain name empty → “Continue”.



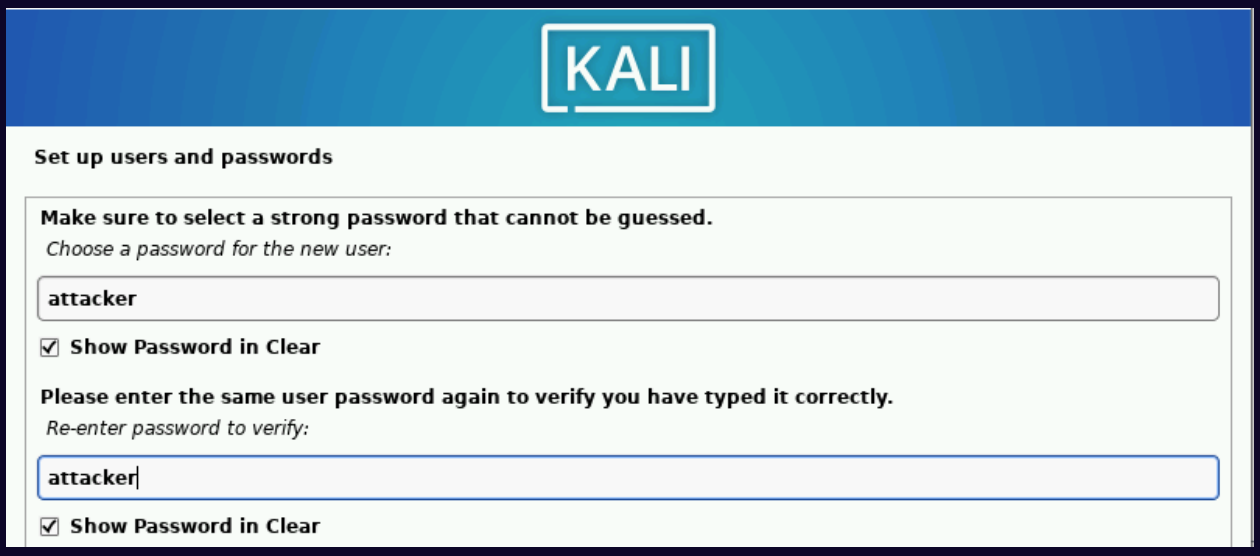
Add “attacker” as the new user and username.





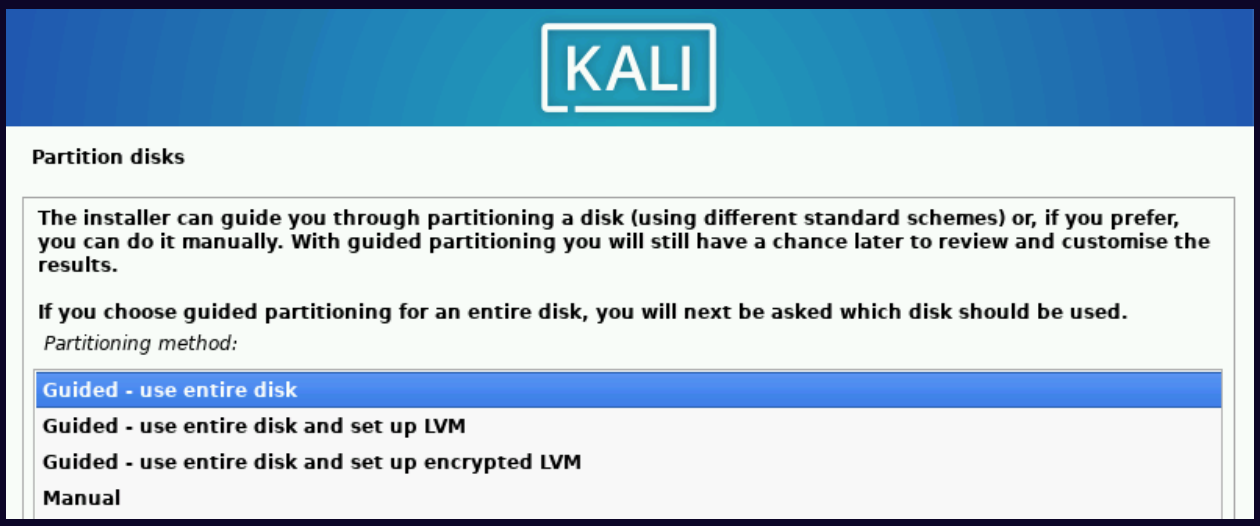
Enter “attacker” as the default password → “Continue”.

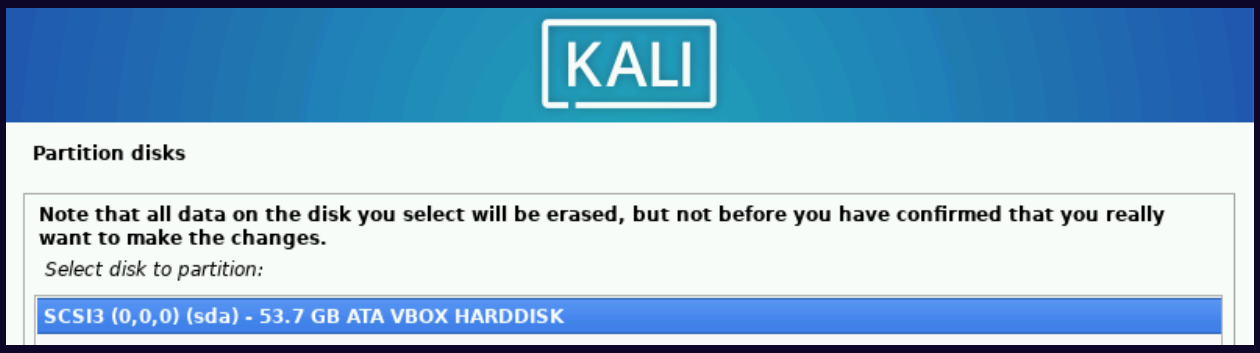
👉 Refer to the “**Project Overview**” guide for more information on default usernames and passwords.

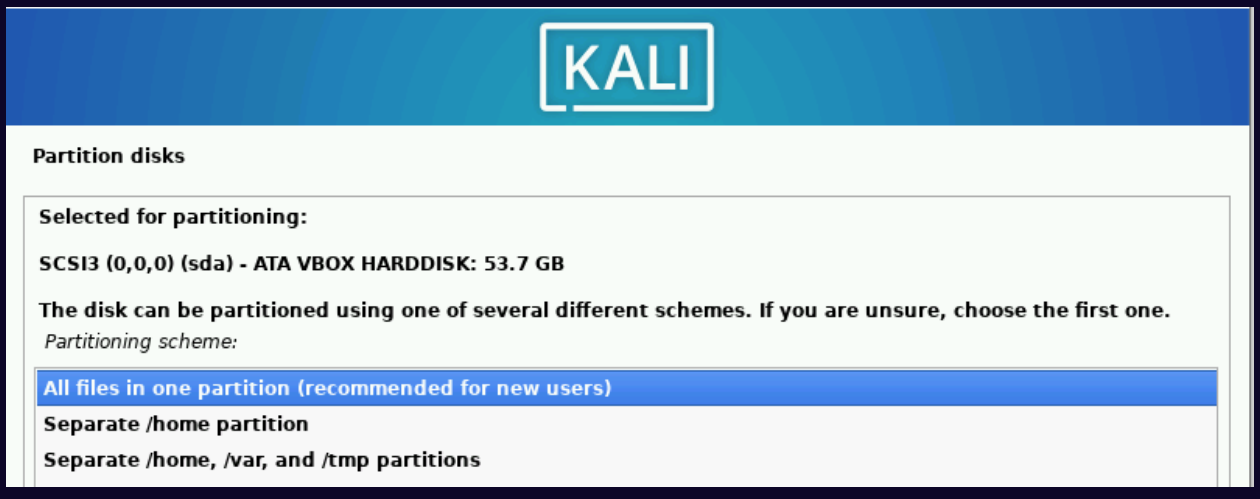


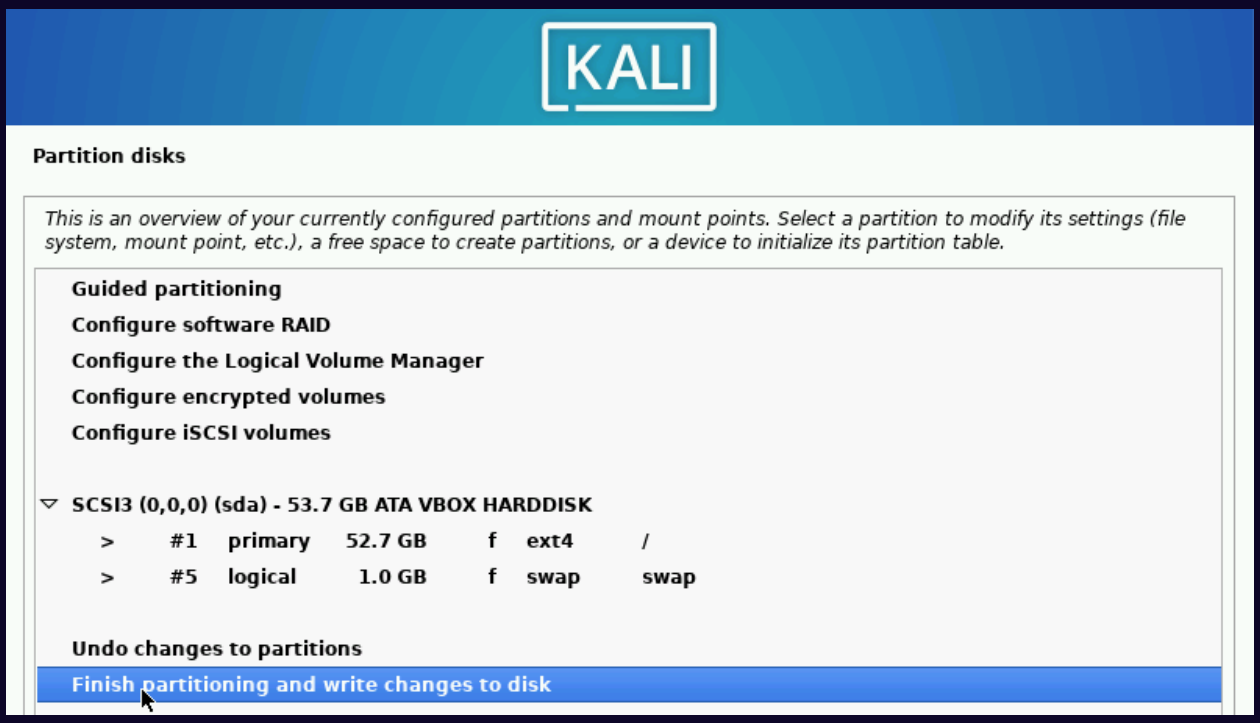
Choose time zone of your choice for the clock option → “Continue.”

Select “Guided – use entire disk” → “Continue.” Keep all defaults selected.

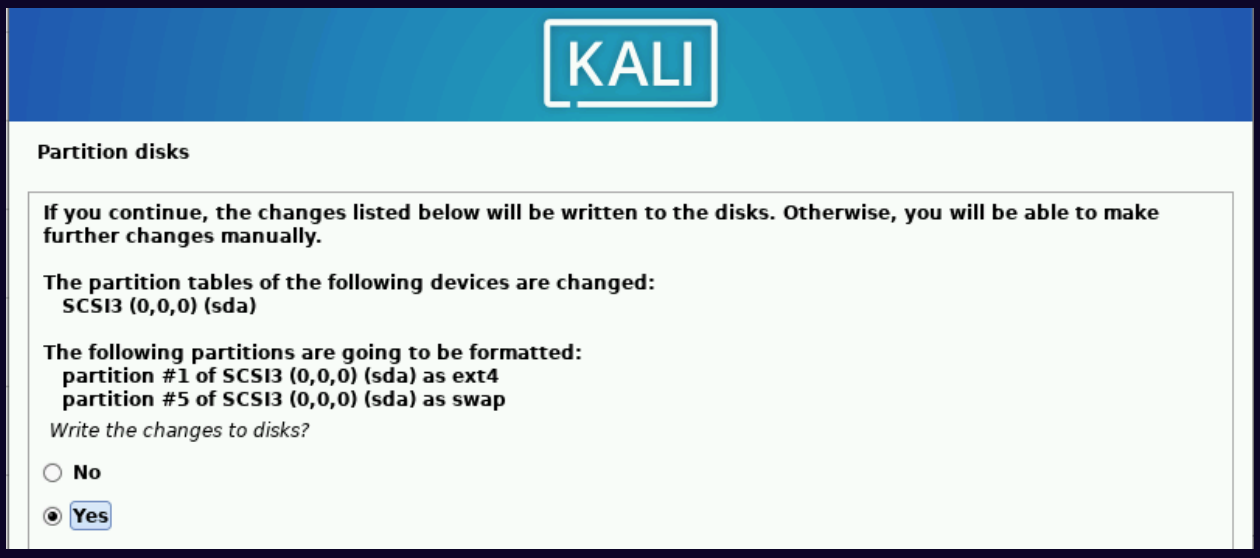

KALI
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk,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


KALI
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) - 53.7 GB ATA VBOX HARDDISK

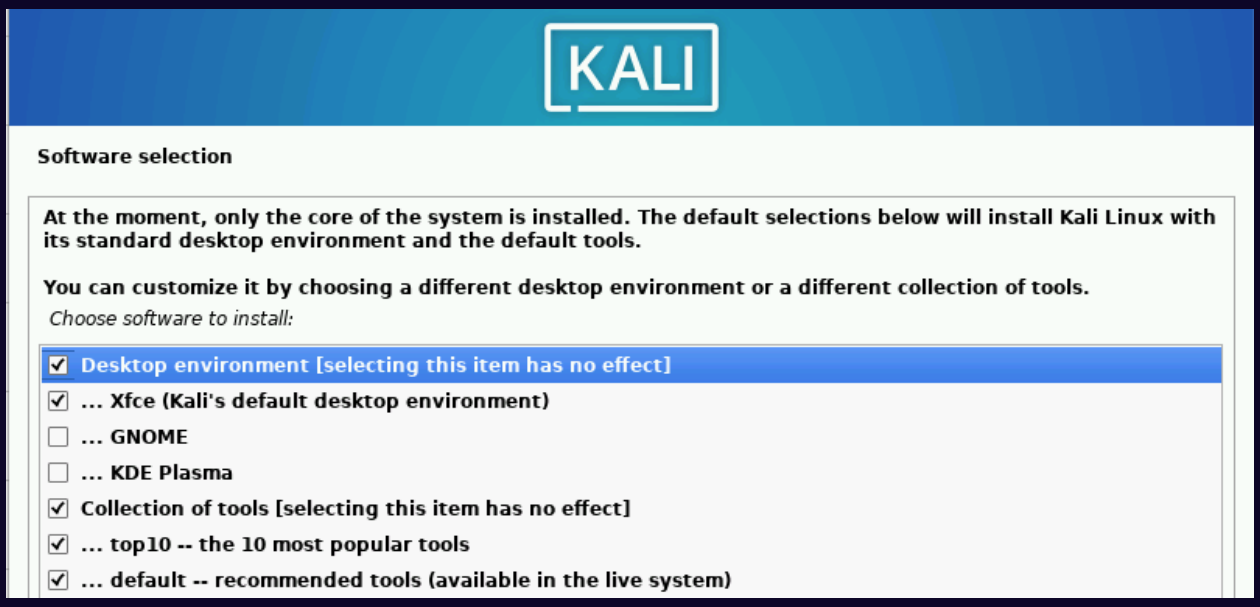

KALI
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 53.7 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions



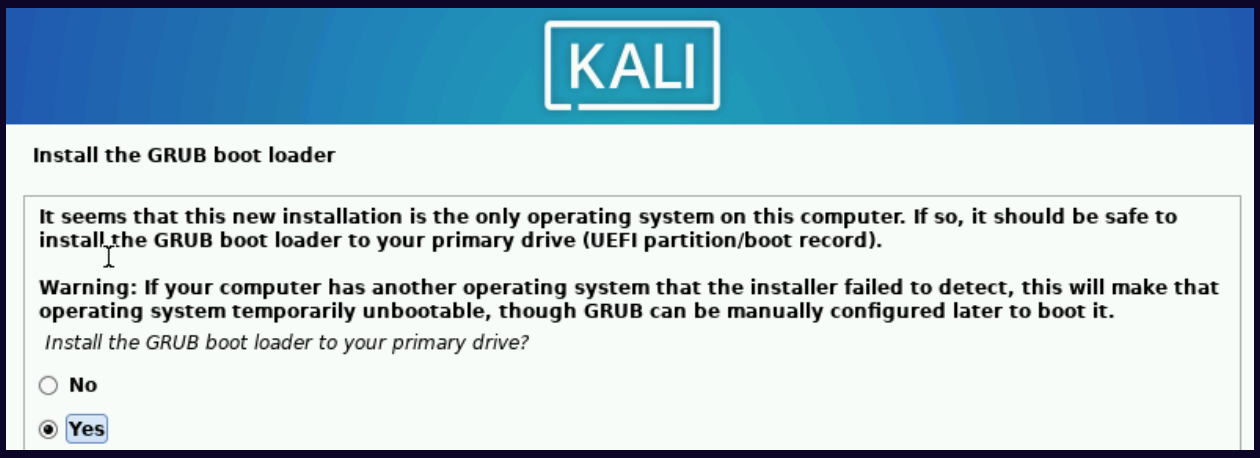
Change “Write the changes to disks?” to “Yes” → “Continue.”

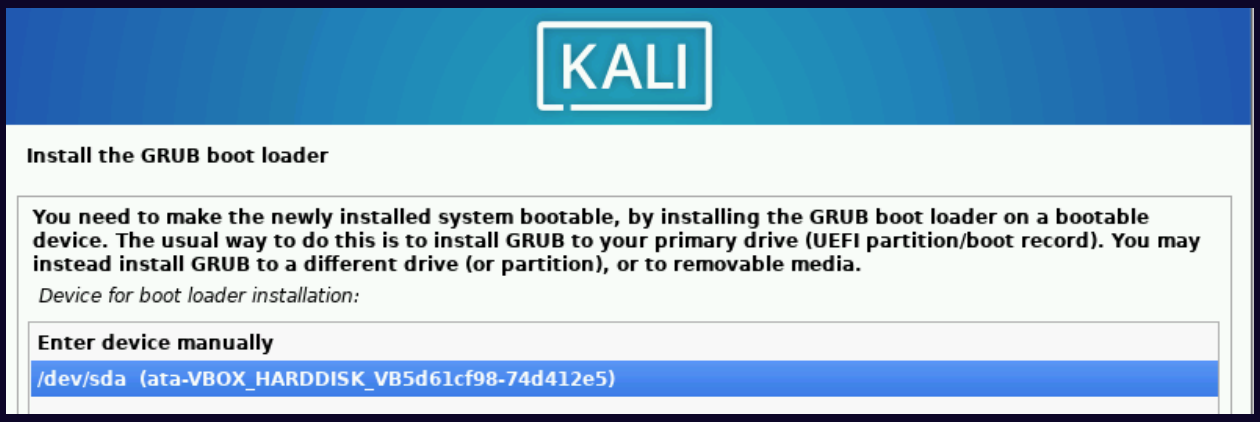


Keep defaults selected → “Continue”. Wait for the software to install.

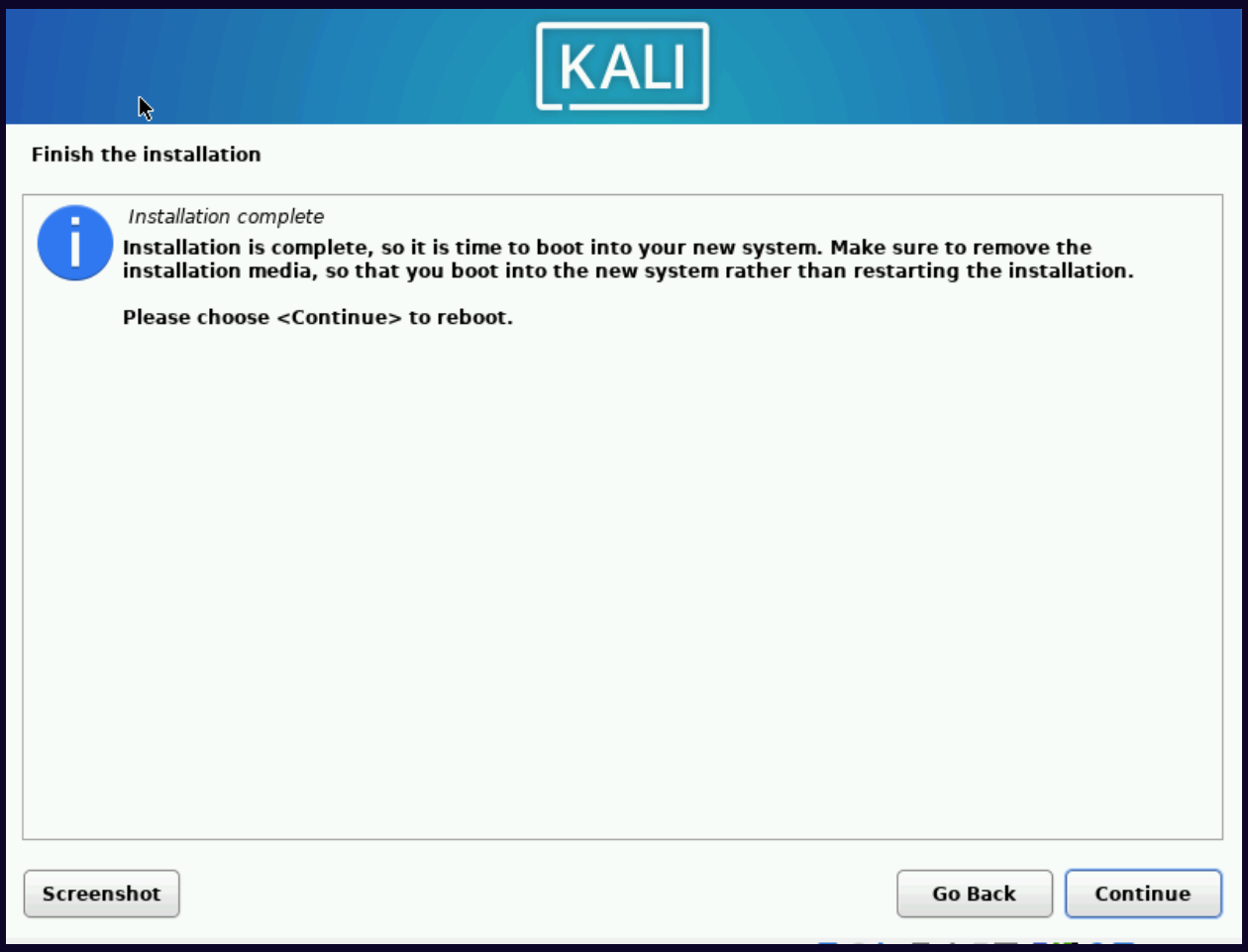


Install the GRUB Loader.

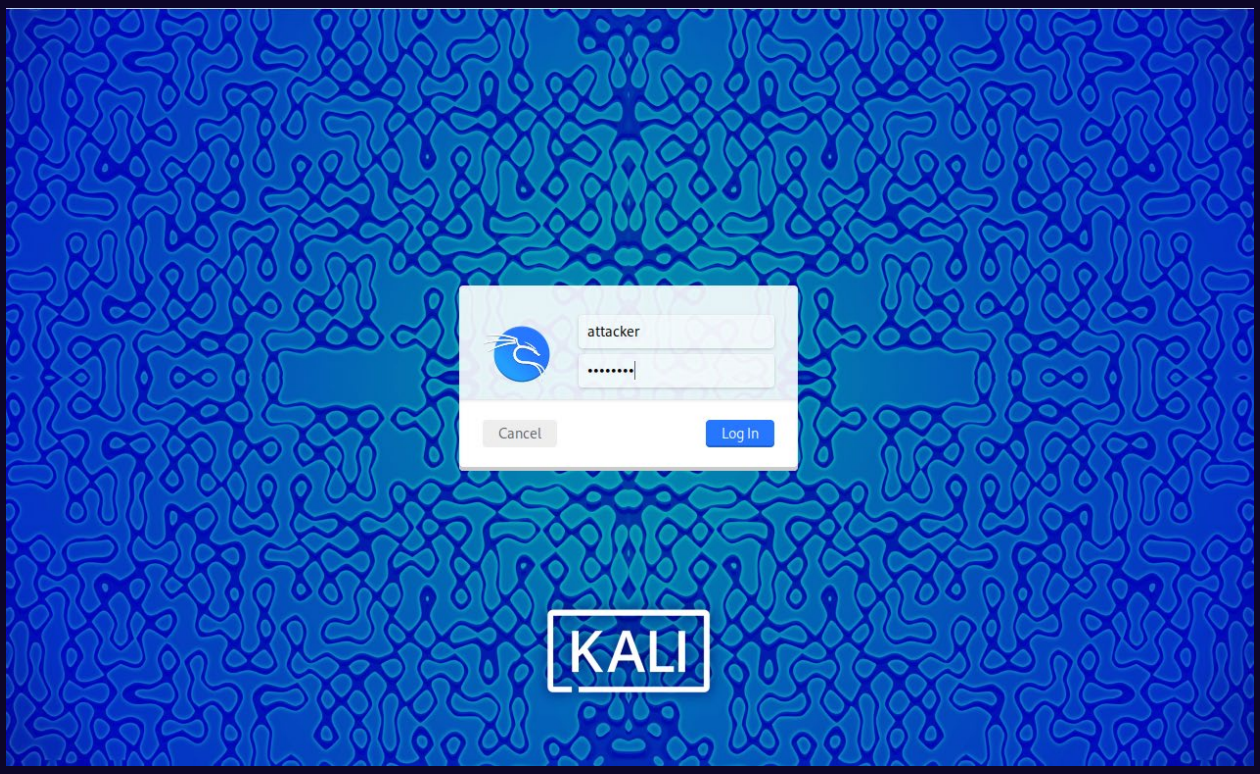




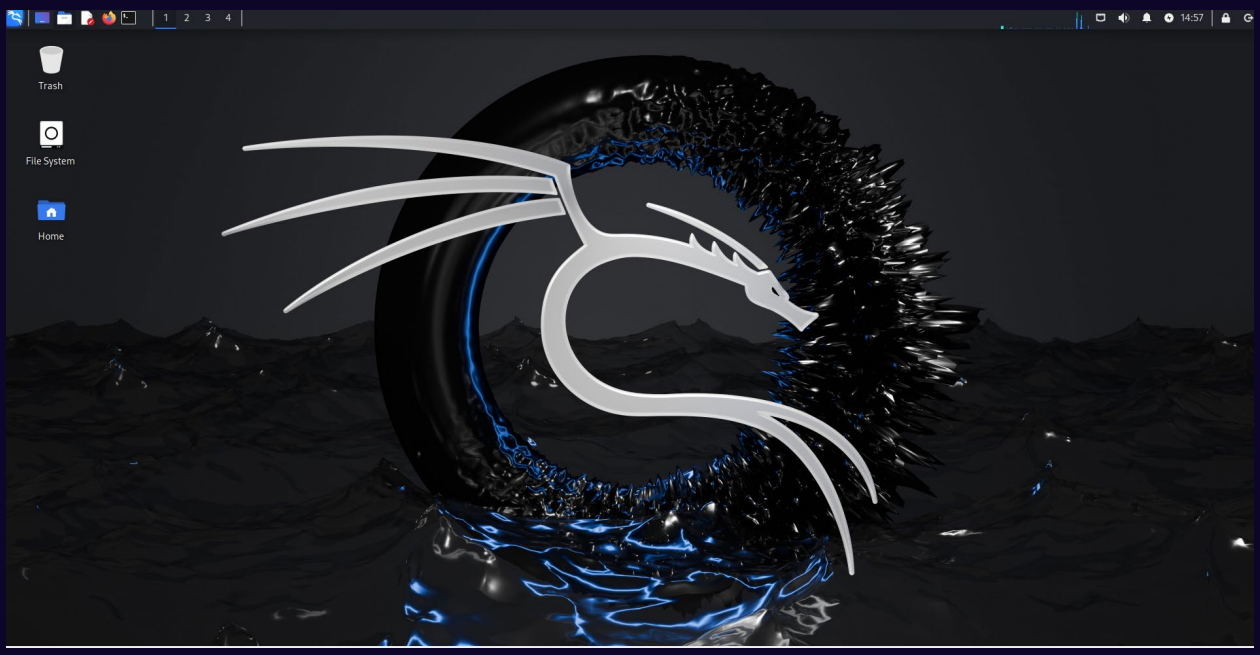
Select “Continue” and allow the system to reboot.



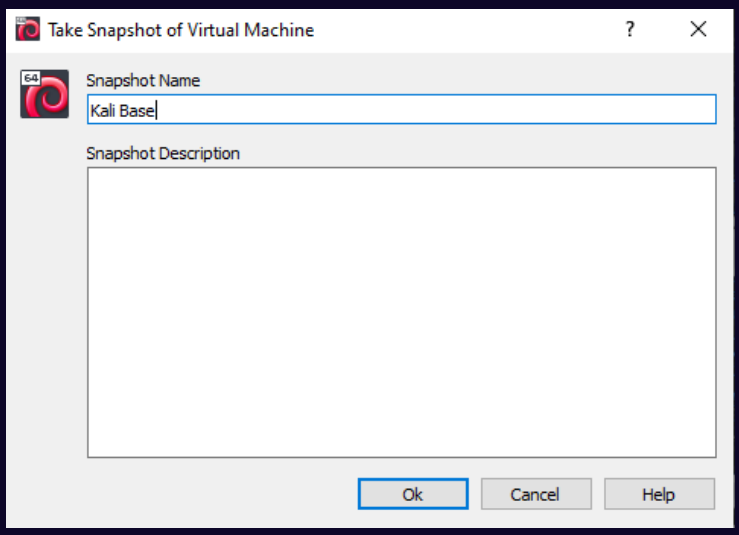
Login as the under the attacker account.



Success!



📸 **Take Snapshot!**

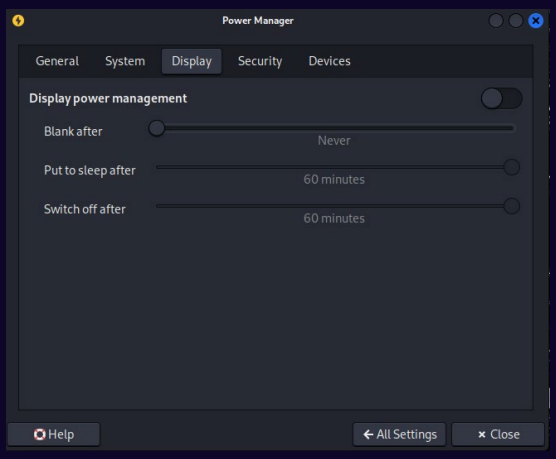


Optional

Disable Default Logoff

Go to the Menu Bar → “Power Manager”.

Navigate to “Display” tab → Drag Toggle to the left.


Power Manager
General
System
Display
Security
Devices
Display power management
Blank after
Never
Put to sleep after
60 minutes
Switch off after
60 minutes
Help
All Settings
Close