Threats and Countermeasures

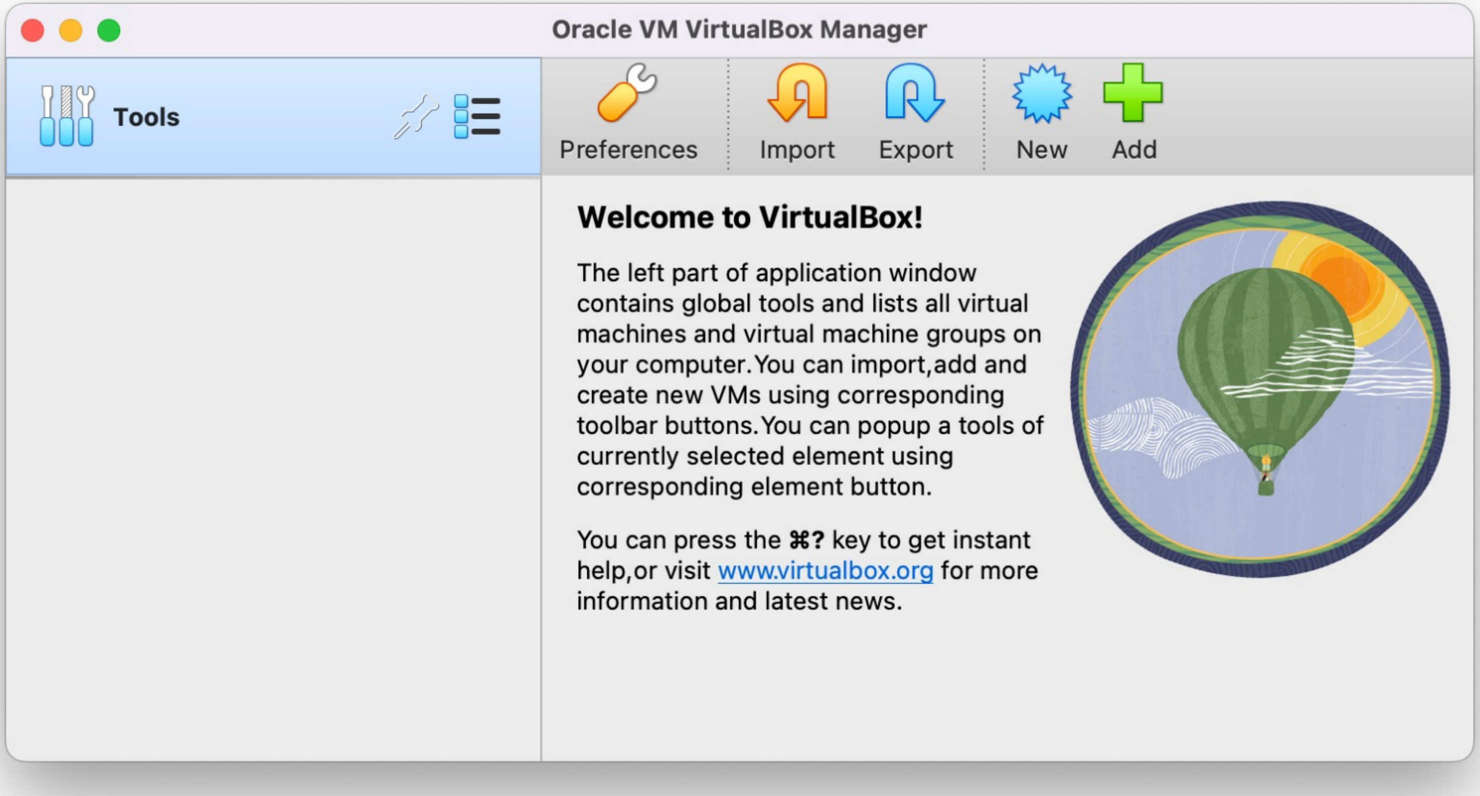
Lecture 01:
Introduction and Setup

COMP-5830/-6830
Spring 2025

Today’s Plan

- Start Kali VM installation
- Course Information
- “Ethical Hacking”
- Finish Kali VM installation
- --- break ---
- Setup Kali VM
- Linux/VM basics
- Linux Hardening

Installing Kali

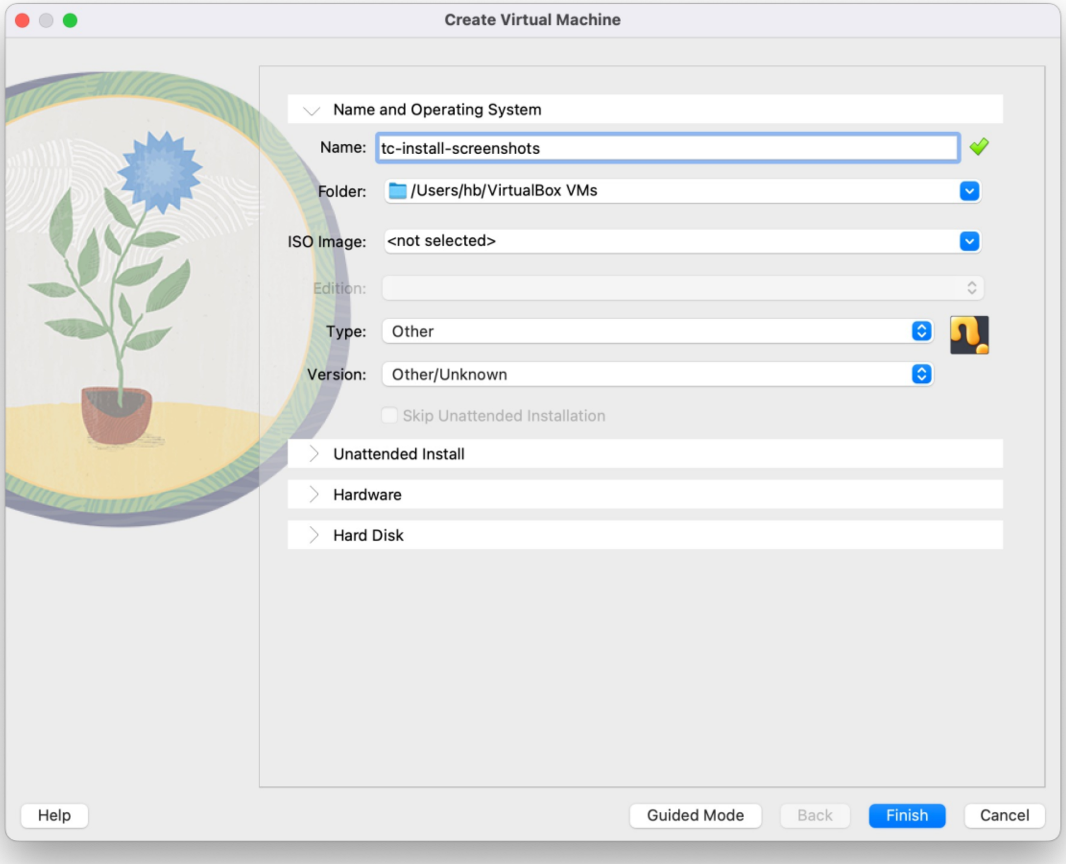


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import,add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **⌘?** key to get instant help,or visit www.virtualbox.org for more information and latest news.

Installing Kali



Create Virtual Machine

Name and Operating System

Name: tc-install-screenshots

Folder: /Users/hb/VirtualBox VMs

ISO Image: <not selected>

Edition:

Type: Other

Version: Other/Unknown

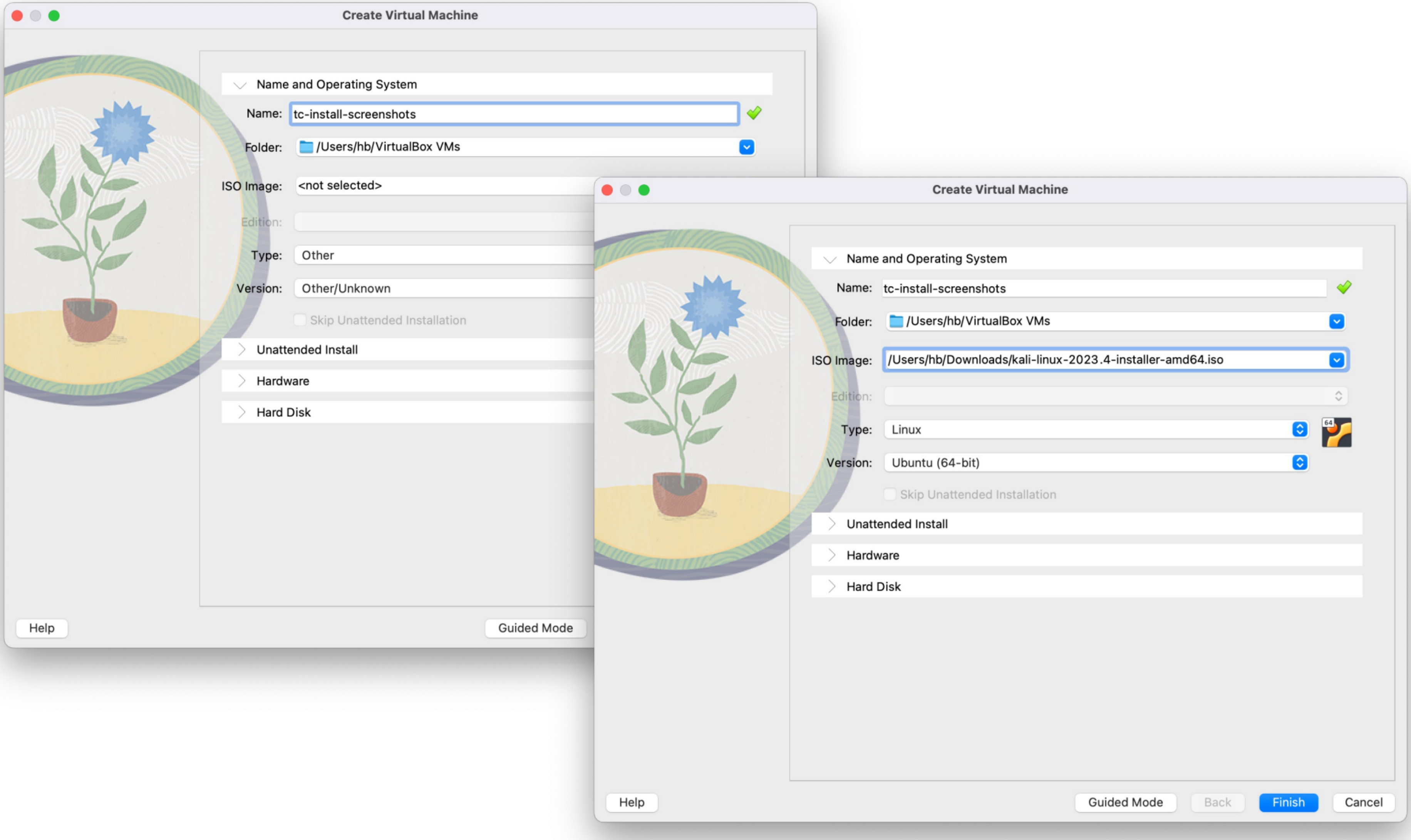
□ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

Installing Kali



Create Virtual Machine

Name and Operating System

Name: tc-install-screenshots

Folder: /Users/hb/VirtualBox VMs

ISO Image: <not selected>

Edition:

Type: Other

Version: Other/Unknown

□ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

Create Virtual Machine

Name and Operating System

Name: tc-install-screenshots

Folder: /Users/hb/VirtualBox VMs

ISO Image: /Users/hb/Downloads/kali-linux-2023.4-installer-amd64.iso

Edition:

Type: Linux

Version: Ubuntu (64-bit)

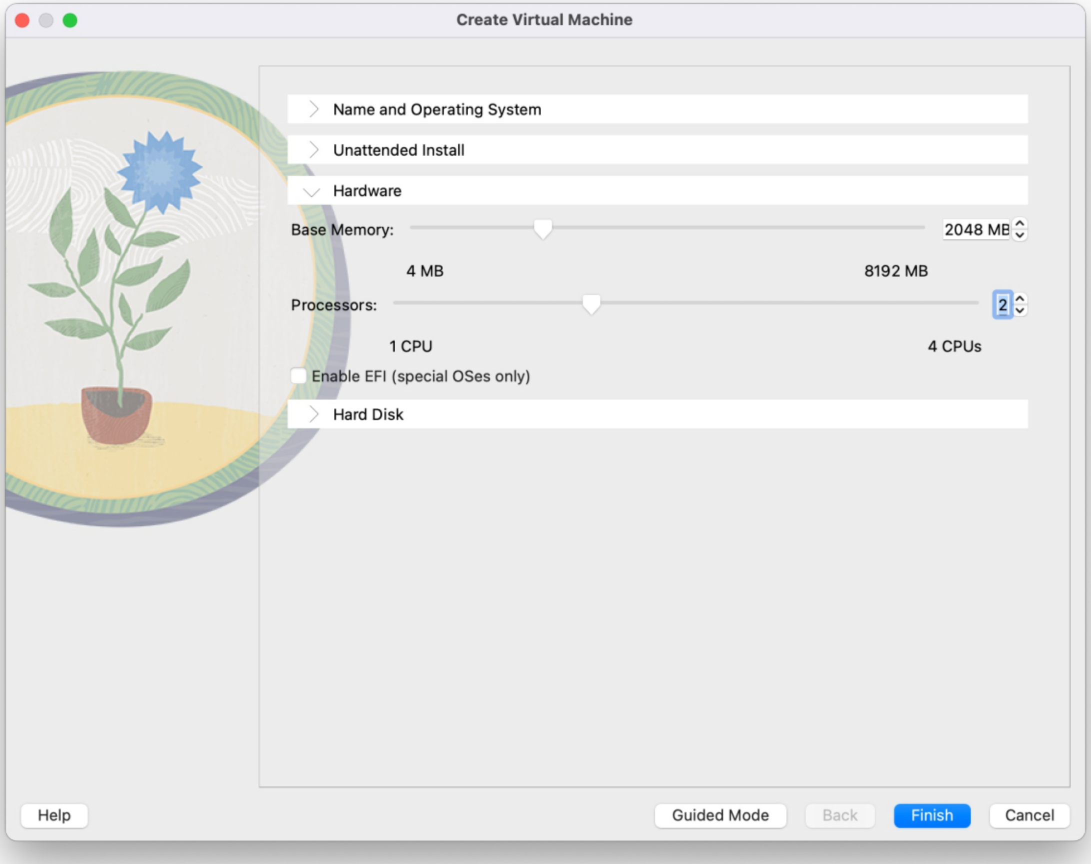
□ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

Installing Kali



Create Virtual Machine

- Name and Operating System
- Unattended Install
- Hardware

Base Memory: 2048 MB

4 MB 8192 MB

Processors: 2

1 CPU 4 CPUs

□ Enable EFI (special OSes only)

- Hard Disk

Threats & Countermeasures

- Very, very different from COMP-5370
  - Hands-on vs Knowledge
  - Concepts vs Implementation

Threats & Countermeasures

- Very, very different from COMP-5370
  - Hands-on vs Knowledge
  - Concepts vs Implementation
- Will rely heavily on common/ready-made tooling and scripts

Threats & Countermeasures

- Very, very different from COMP-5370
  - Hands-on vs Knowledge
  - Concepts vs Implementation

- Will rely heavily on common/ready-made tooling and scripts

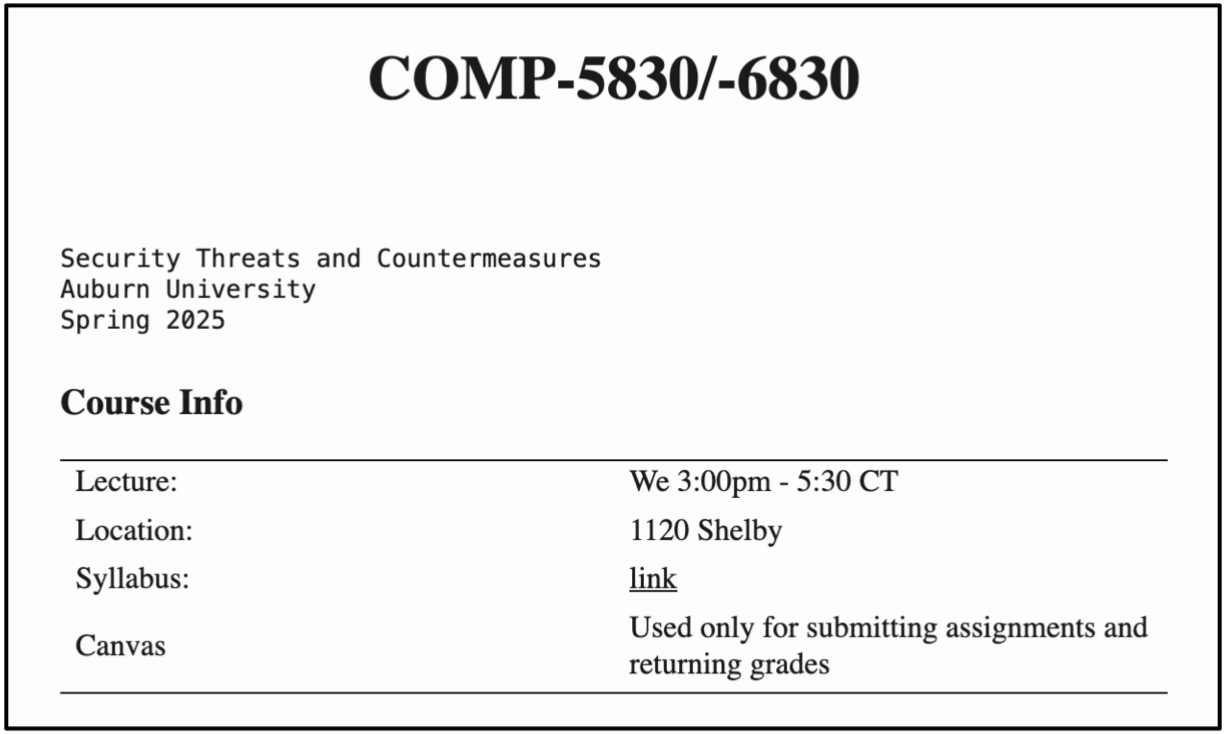
TOOLS CHANGE OVER TIME BUT TECHNIQUES STAY THE SAME

Learning Objectives

- Identify and apply each step of the ethical hacking process
- Given a network configuration, properly identify running systems and services
- Conduct research and properly identify system and service vulnerabilities
- Properly select and use security tools
- For a given vulnerability, recommend effective security controls

Course Website

https://comp5830.org/



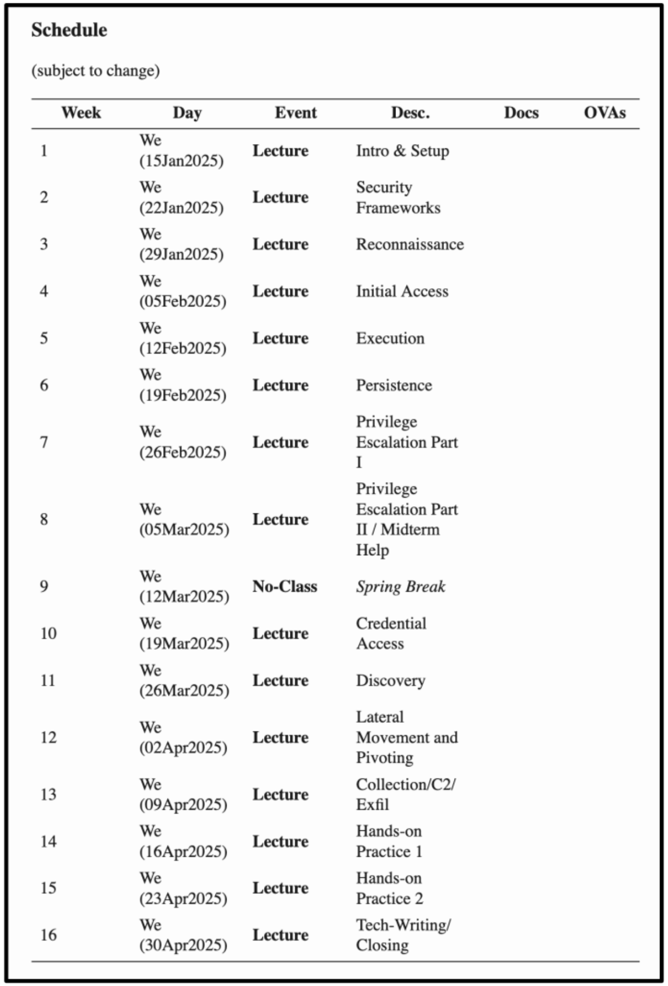
COMP-5830/-6830

```
Security Threats and Countermeasures
Auburn University
Spring 2025
```

Course Info

Lecture:	We 3:00pm - 5:30 CT
Location:	1120 Shelby
Syllabus:	link
Canvas	Used only for submitting assignments and returning grades

Schedule

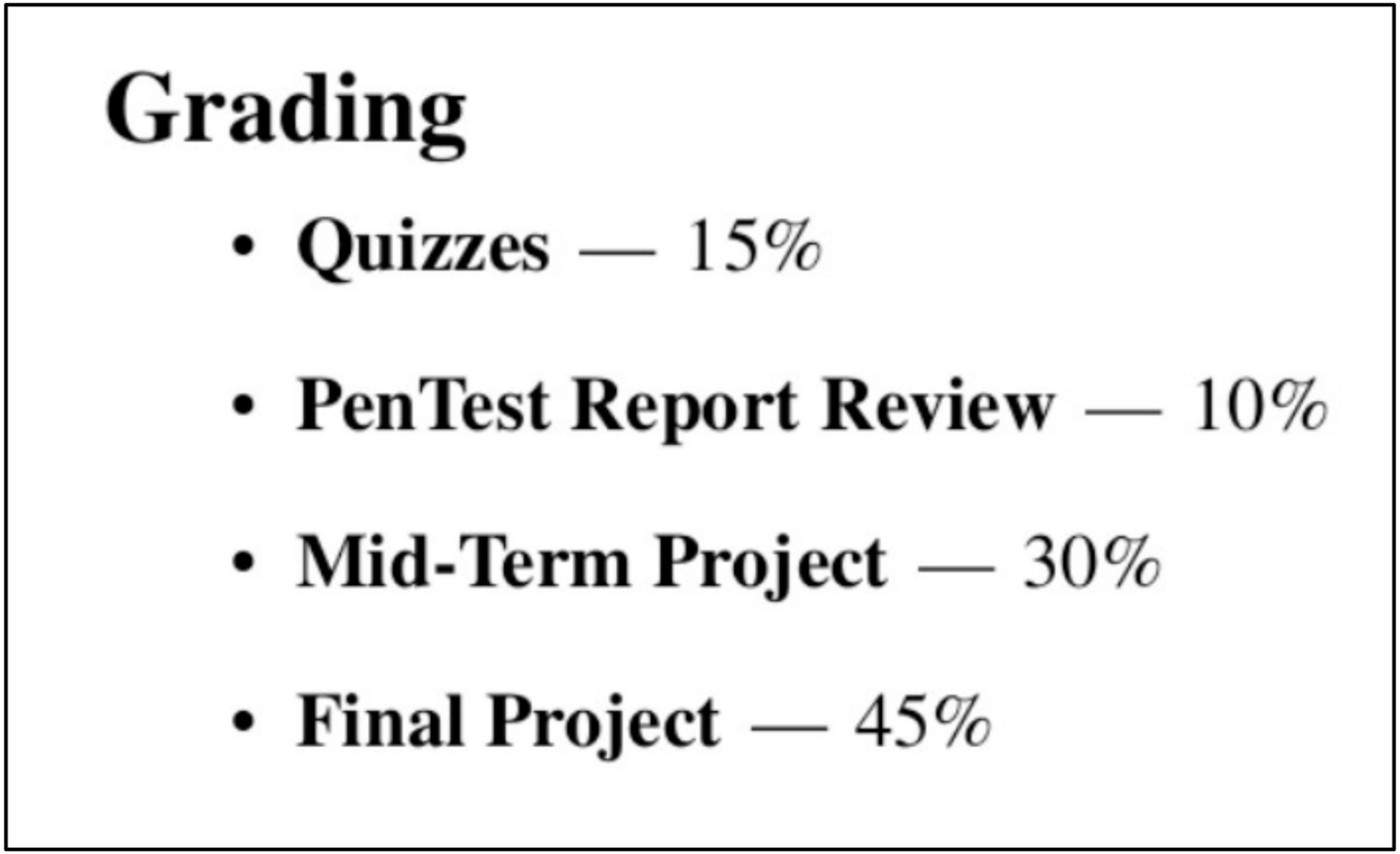


Schedule

(subject to change)

Week	Day	Event	Desc.	Docs	OVAs
1	We (15Jan2025)	**Lecture**	Intro & Setup		
2	We (22Jan2025)	**Lecture**	Security Frameworks		
3	We (29Jan2025)	**Lecture**	Reconnaissance		
4	We (05Feb2025)	**Lecture**	Initial Access		
5	We (12Feb2025)	**Lecture**	Execution		
6	We (19Feb2025)	**Lecture**	Persistence		
7	We (26Feb2025)	**Lecture**	Privilege Escalation Part I		
8	We (05Mar2025)	**Lecture**	Privilege Escalation Part II / Midterm Help		
9	We (12Mar2025)	**No-Class**	*Spring Break*		
10	We (19Mar2025)	**Lecture**	Credential Access		
11	We (26Mar2025)	**Lecture**	Discovery		
12	We (02Apr2025)	**Lecture**	Lateral Movement and Pivoting		
13	We (09Apr2025)	**Lecture**	Collection/C2/Exfil		
14	We (16Apr2025)	**Lecture**	Hands-on Practice 1		
15	We (23Apr2025)	**Lecture**	Hands-on Practice 2		
16	We (30Apr2025)	**Lecture**	Tech-Writing/Closing		

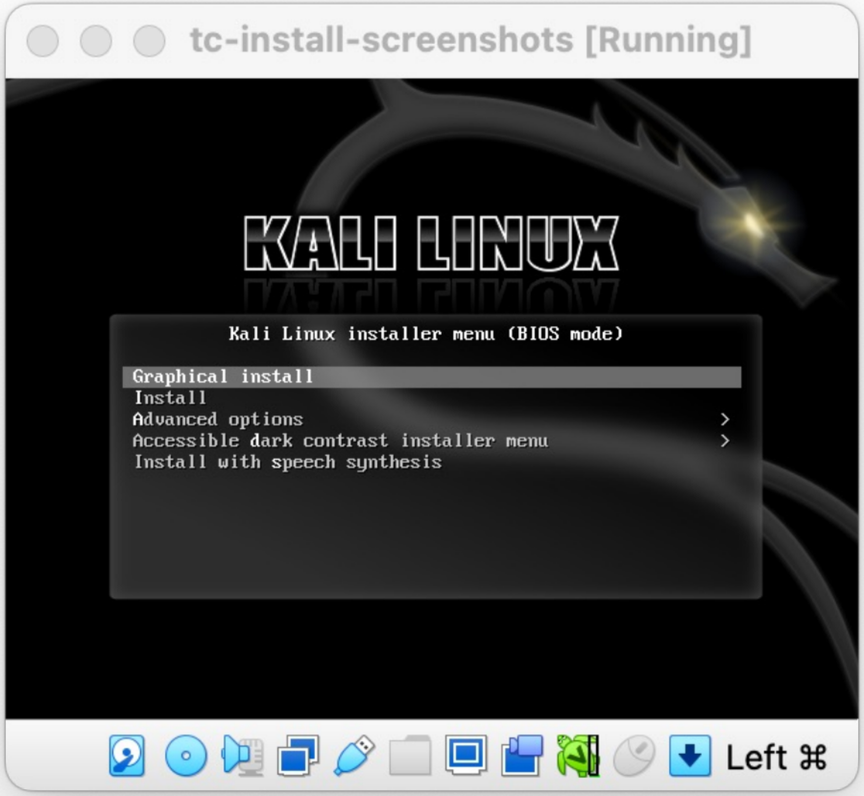
Grading



Grading

- Quizzes — 15%
- PenTest Report Review — 10%
- Mid-Term Project — 30%
- Final Project — 45%

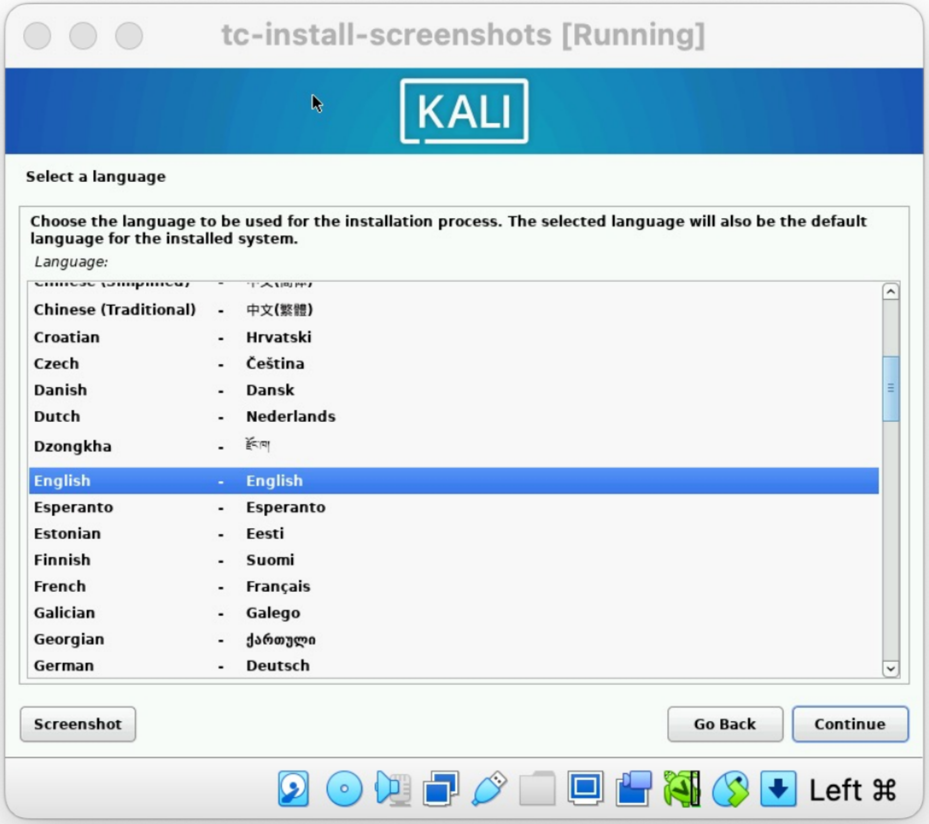
Installing Kali



Kali Linux installer menu (BIOS mode)

```
Graphical install
Install
Advanced options                                            >
Accessible dark contrast installer menu                     >
Install with speech synthesis
```

Installing Kali



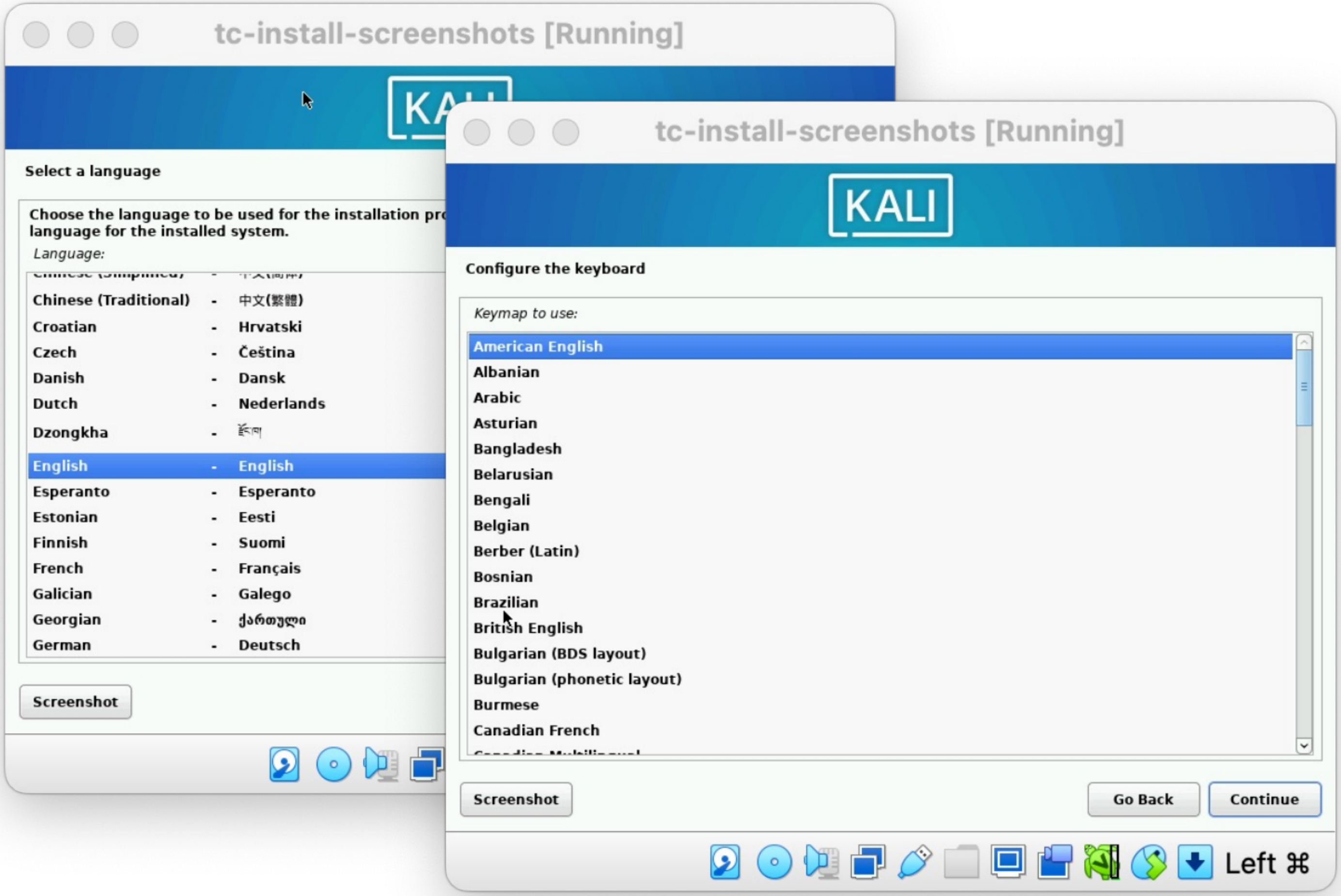
Select a language

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

Installing Kali



tc-install-screenshots [Running]

Select a language

Choose the language to be used for the installation pr
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

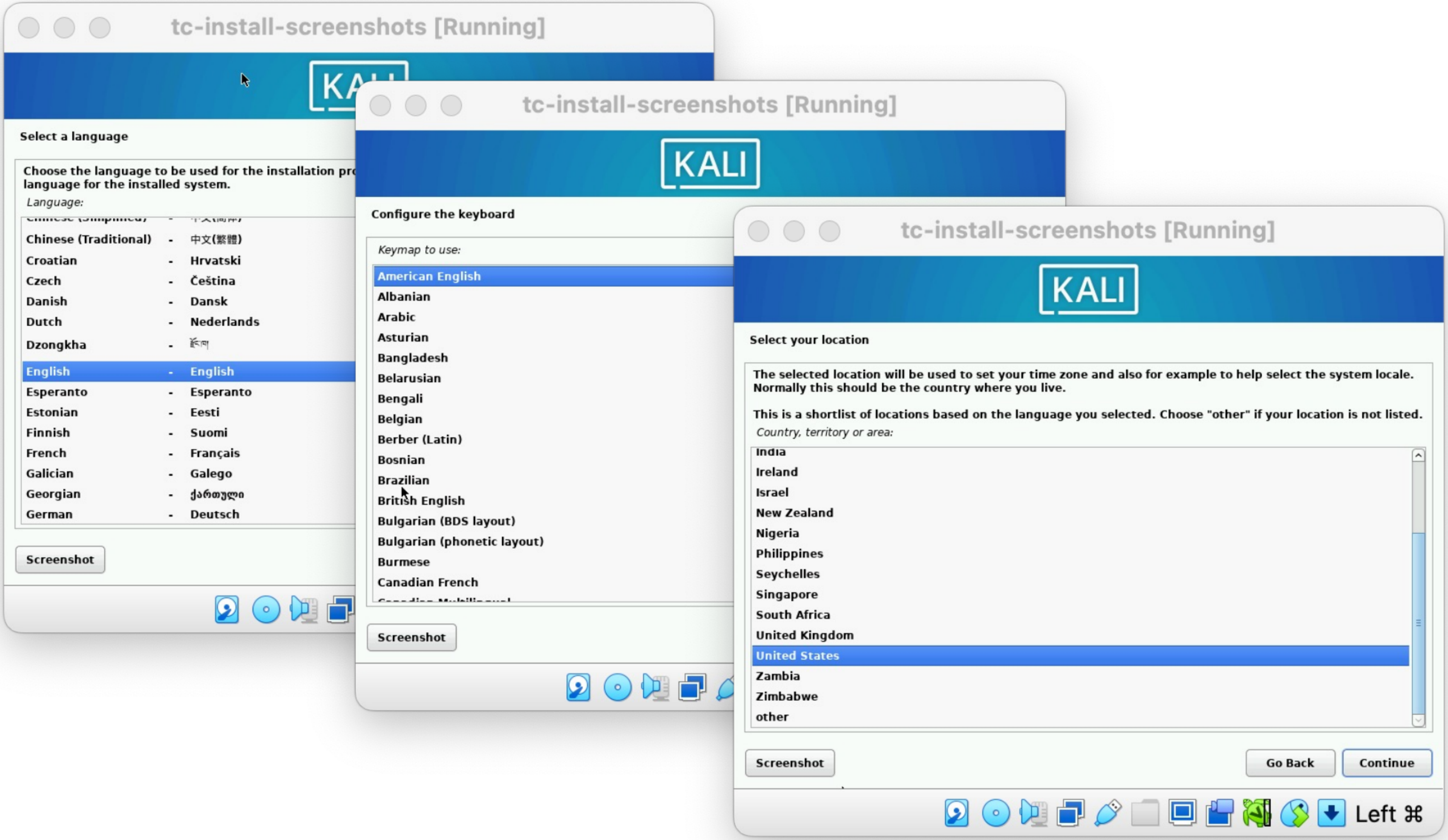
tc-install-screenshots [Running]

Configure the keyboard

Keymap to use:

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

Installing Kali



Select a language

Choose the language to be used for the installation pr
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

Configure the keyboard

Keymap to use:

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

Select your location

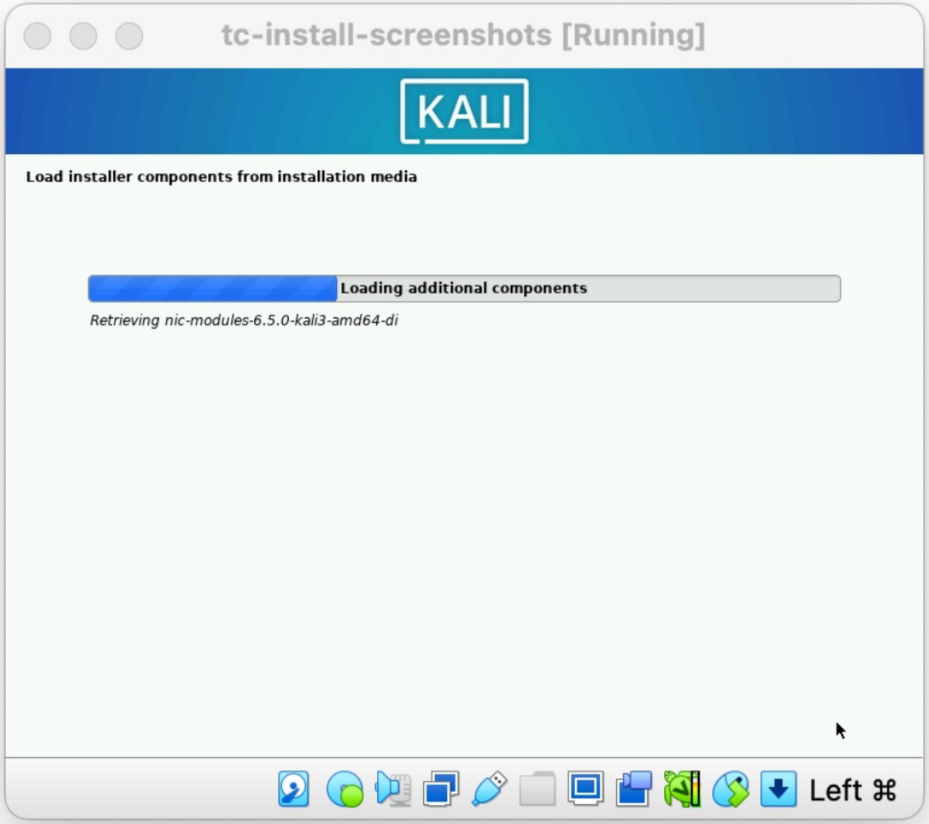
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

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

Country, territory or area:

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

Installing Kali

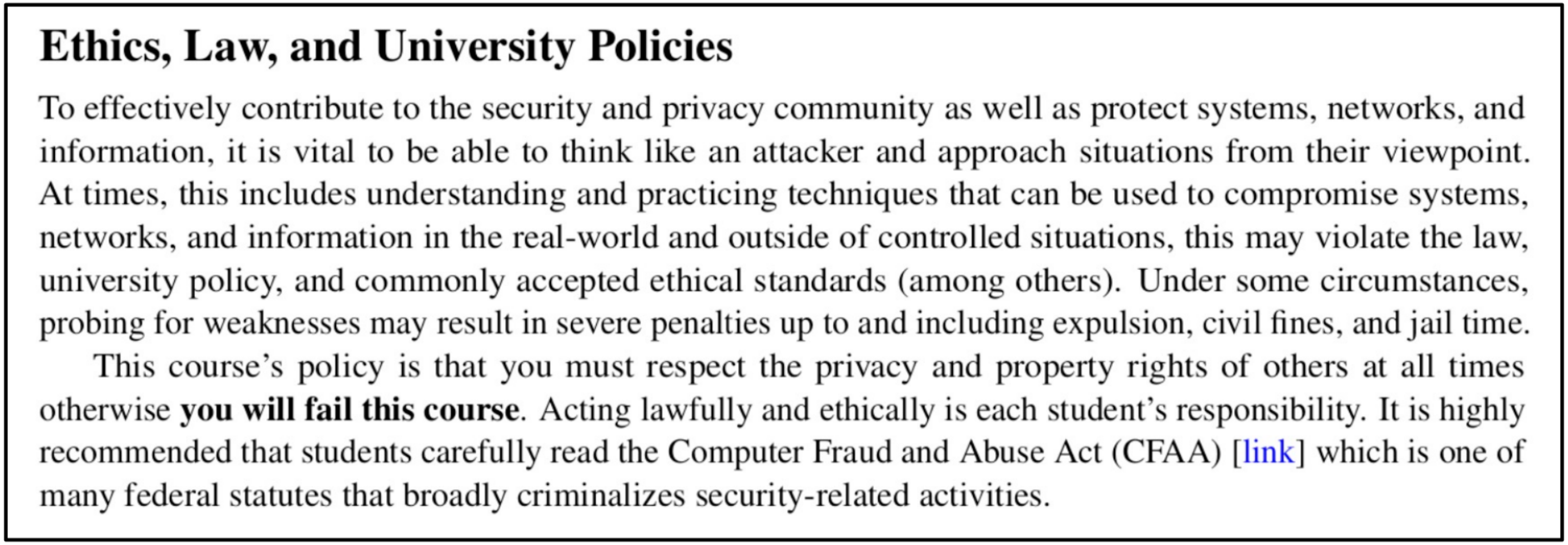


Load installer components from installation media

Loading additional components

Retrieving nic-modules-6.5.0-kali3-amd64-di

DO NOT BREAK THE LAW



Ethics, Law, and University Policies

To effectively contribute to the security and privacy community as well as protect systems, networks, and information, it is vital to be able to think like an attacker and approach situations from their viewpoint. At times, this includes understanding and practicing techniques that can be used to compromise systems, networks, and information in the real-world and outside of controlled situations, this may violate the law, university policy, and commonly accepted ethical standards (among others). Under some circumstances, probing for weaknesses may result in severe penalties up to and including expulsion, civil fines, and jail time.

This course's policy is that you must respect the privacy and property rights of others at all times otherwise **you will fail this course**. Acting lawfully and ethically is each student's responsibility. It is highly recommended that students carefully read the Computer Fraud and Abuse Act (CFAA) [link] which is one of many federal statutes that broadly criminalizes security-related activities.

Law/Ethics/University Policy

- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

Law/Ethics/University Policy

- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

1) DO NOT COMMIT CRIMES

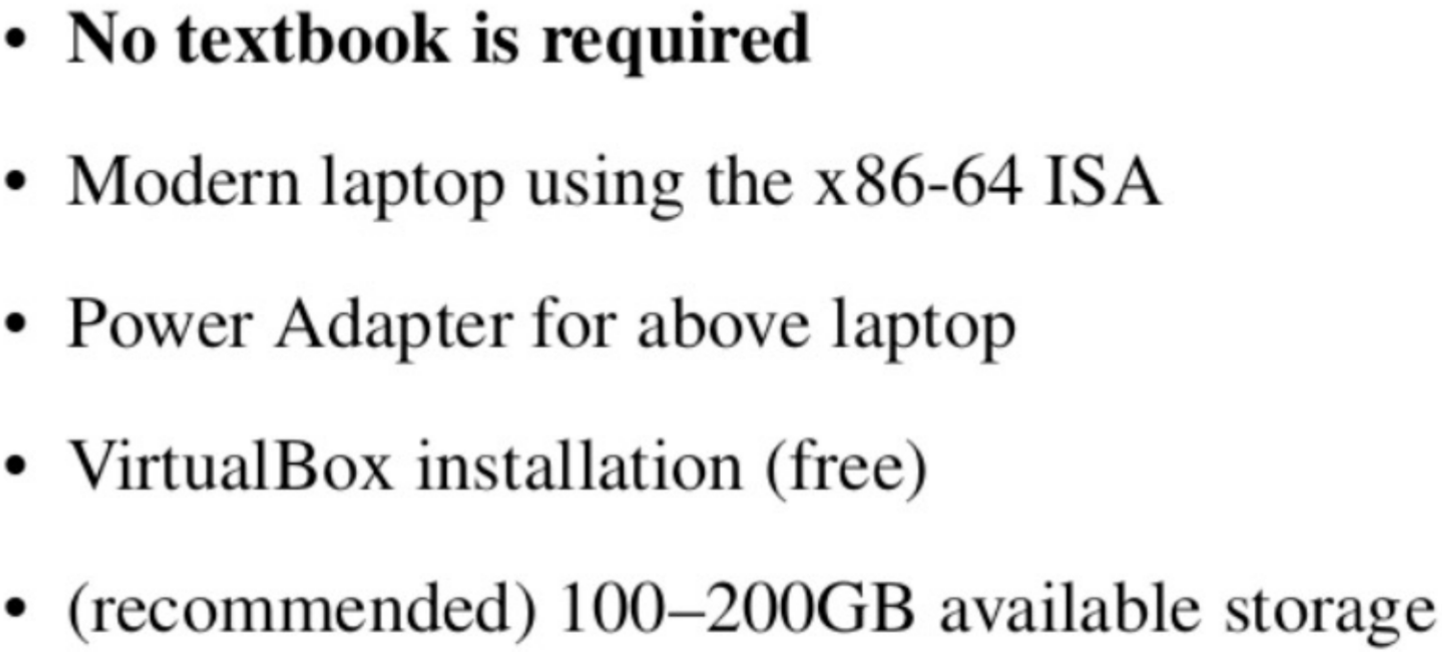
Law/Ethics/University Policy

- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

1) DO NOT COMMIT CRIMES

2) Respect others' security & privacy

Materials



- **No textbook is required**
- Modern laptop using the x86-64 ISA
- Power Adapter for above laptop
- VirtualBox installation (free)
- (recommended) 100–200GB available storage

Materials

- **No textbook is required**
- Modern laptop using the x86-64 ISA
- Power Adapter for above laptop
- VirtualBox installation (free)
- (recor led) 100–200GB ble storage

THE HACKER PLAYBOOK 2
Practical Guide To Penetration Testing
RTFM
Red Team Field Manual
Attacking Network Protocols
A Hacker's Guide to Capture, Analysis, and Exploitation
James Forshaw

BTFM
Blue Team Field Manual
Hussam Khrais
Python for Offensive PenTest
A practical guide to ethical hacking and penetration testing using Python
Packt
THE HACKER PLAYBOOK 3
Practical Guide To Penetration Testing

News & Other Resources

- ThreatPost
- Krebs on Security
- DarkReading
- Wired
- SANS Reading Room
- Hacker News
- MIT Technology Review

Other Practice Resources

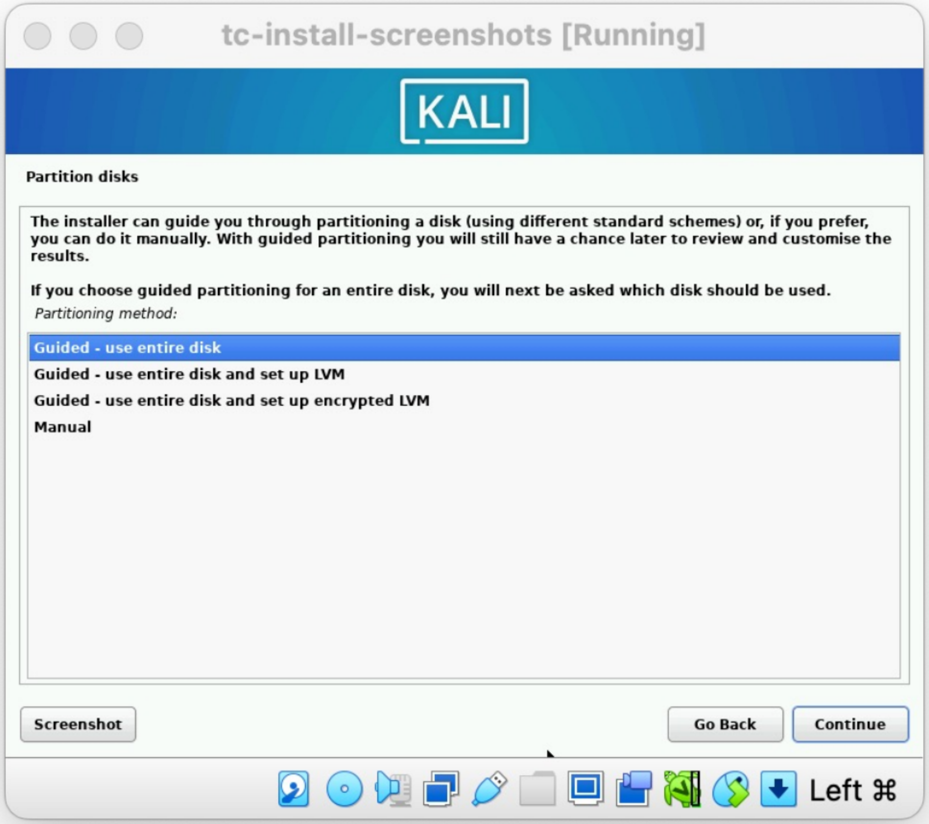
- HackTheBox
- Pentester Academy
- TryHackMe
- Over The Wire
- Ethical Hacking Repository

Have Questions?

- In-person interaction usually solve problems immediately
  - Office hours in syllabus and on website
  - After-class, open-door, etc. (instructor-only)
  - If the office-phone rings, I pick it up

- Email is a valid but highly-latent channel
  - Might answer in next lecture
  - Might take couple of days to get to your email

Installing Kali



Partition disks

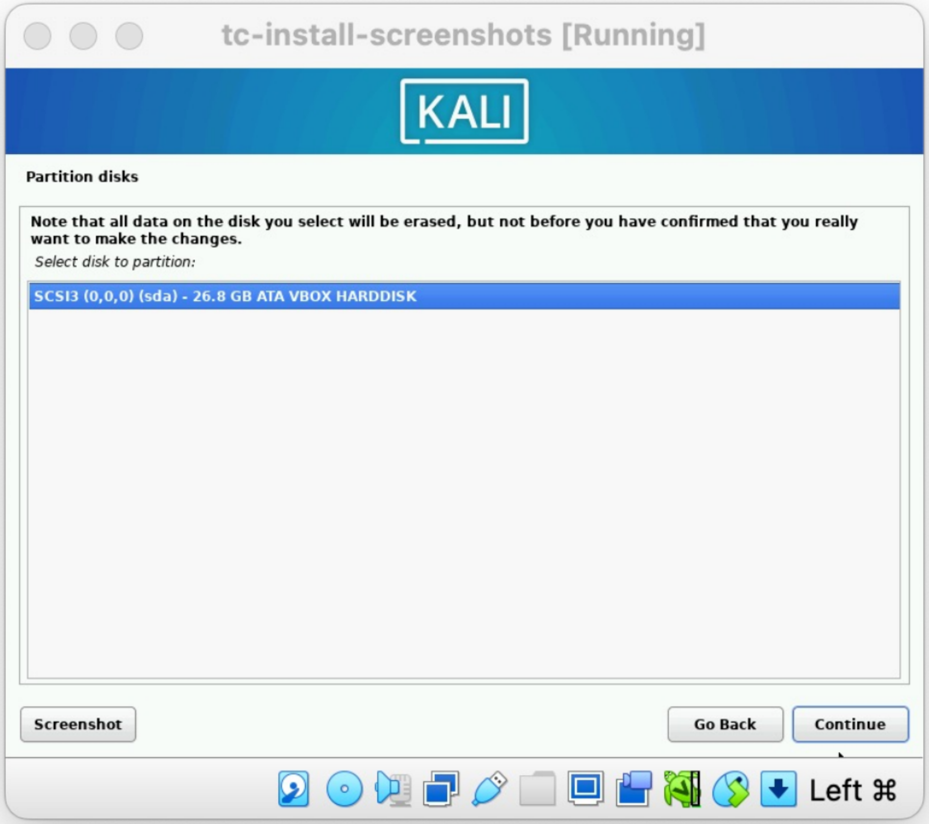
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

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

Installing Kali



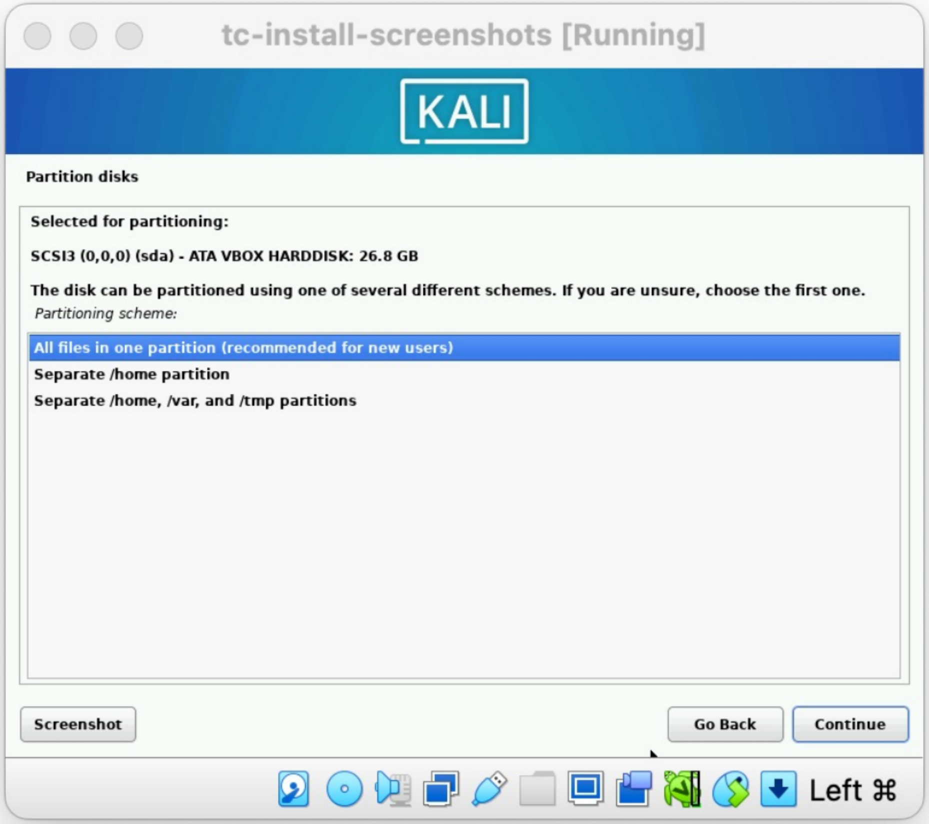
Partition disks

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) - 26.8 GB ATA VBOX HARDDISK

Installing Kali



Partition disks

Selected for partitioning:

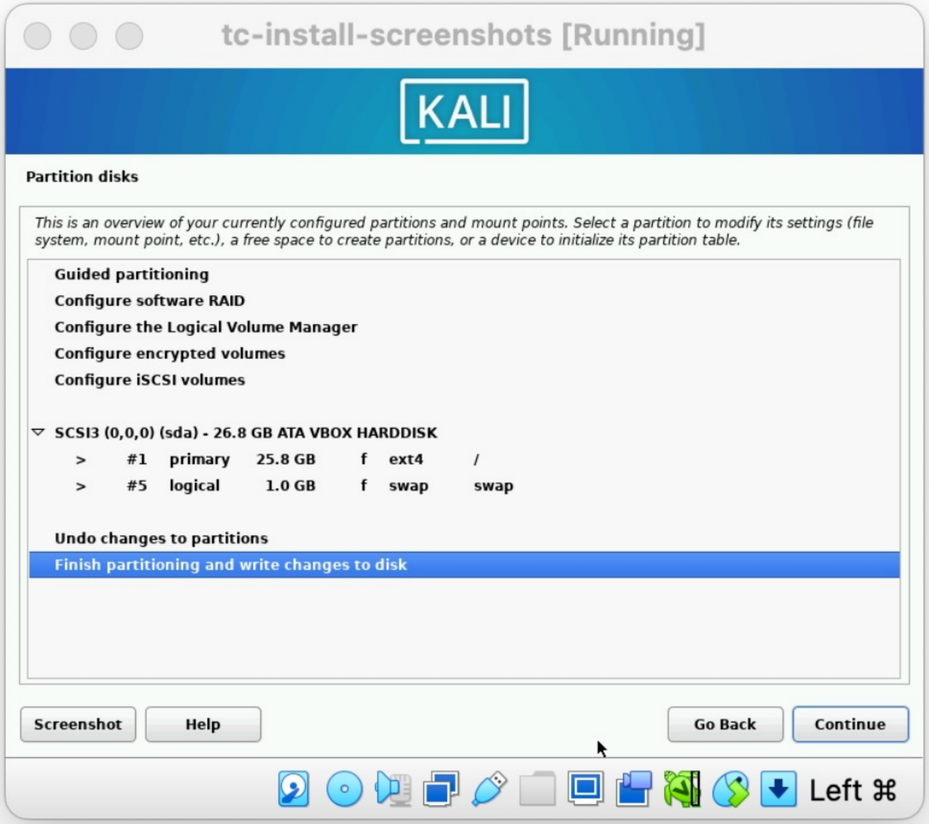
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 26.8 GB

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

Installing Kali



Partition disks

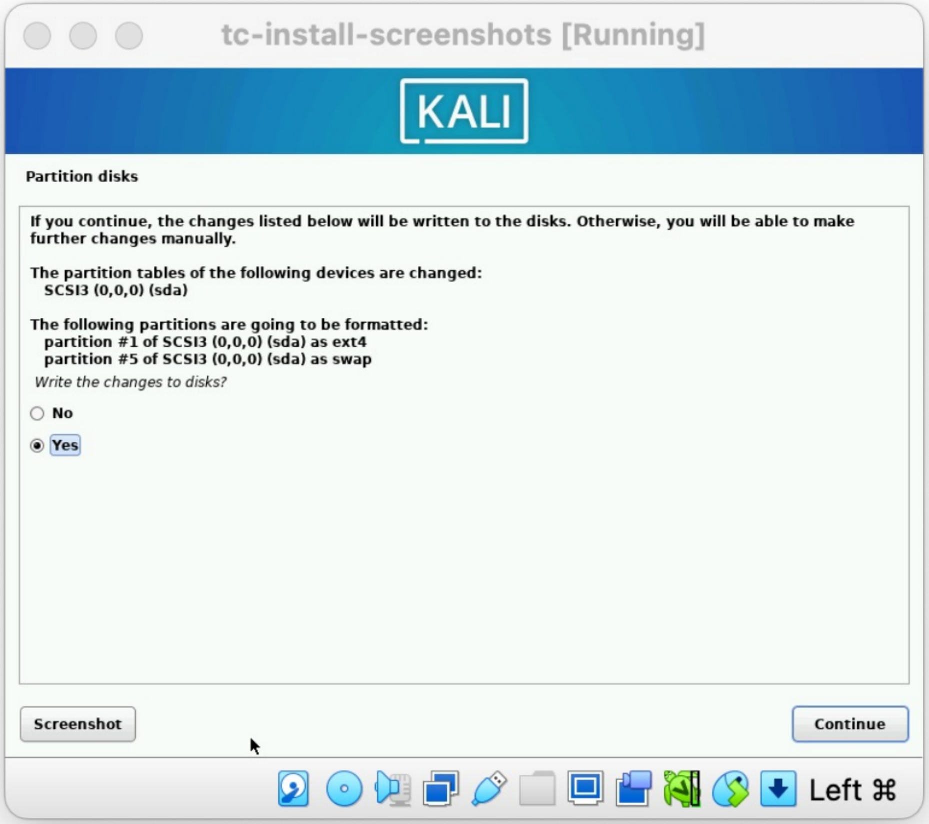
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

```
▽ SCSI3 (0,0,0) (sda) - 26.8 GB ATA VBOX HARDDISK
    >   #1   primary    25.8 GB   f   ext4    /
    >   #5   logical     1.0 GB   f   swap    swap
```

Undo changes to partitions
Finish partitioning and write changes to disk

Installing Kali



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:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

○ No

● Yes

Adversary

- Intelligent Actor
  - Person, Group, or Organization
- Have own:
  - Capabilities
  - Motivations
  - Intentions
- Are **NOT** restricted by expectations

Role-Playing as "Bad Guys"

Security Mindset

A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
  - Comprehend abilities and behavior patterns
  - Understand how search for/exploit weaknesses
- Have to think like a defender
  - Identify what is being protected against who
  - Analyze/Evaluate cost-benefit trade-offs

Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”

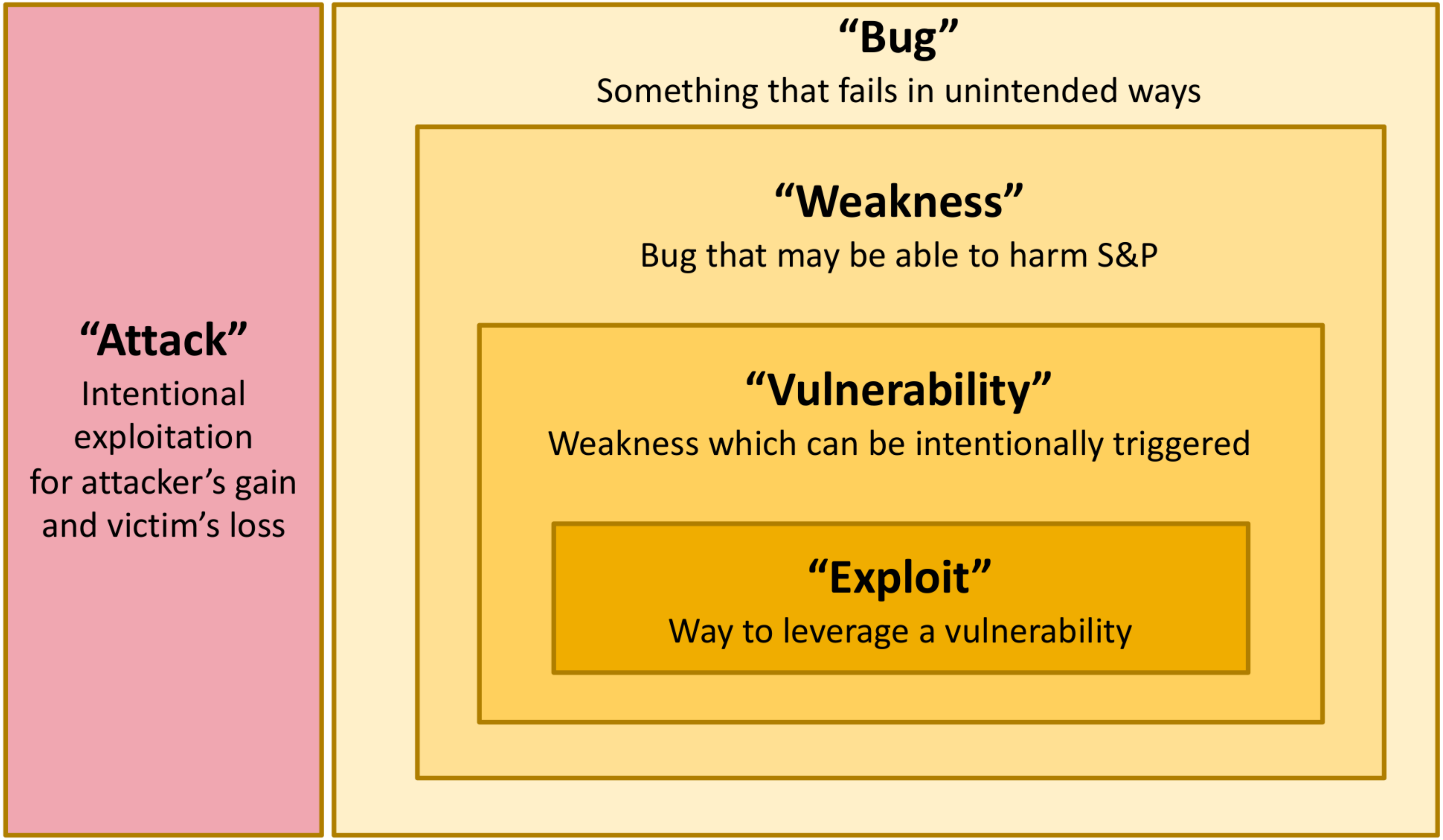
Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
  - What are the creator’s expectations?
  - Who else does the creator rely on?

Thinking Like an Attacker

- What is the **easiest/simplest** way to win?
  - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
  - What are the creator’s expectations?
  - Who else does the creator rely on?
- What are the **implicit assumptions** which the aren’t always true/strong?
  - “outside the box” solutions

Security Vocabulary



“Attack”

Intentional exploitation for attacker’s gain and victim’s loss

“Bug”

Something that fails in unintended ways

“Weakness”

Bug that may be able to harm S&P

“Vulnerability”

Weakness which can be intentionally triggered

“Exploit”

Way to leverage a vulnerability

Security Vocabulary is HARD

Security
Privacy
Resilience
Information Assurance
Risk Management
C---r + *any of above*

- Everyone has a specific definition for every word
  - Not all definitions agree
- Definitions change frequently and new words are constantly added to vocabulary

Hacker "Types"

- System Hacker vs. System Cracker
- White Hat
- Black Hat
- Gray Hat
- Script Kiddies
- Cyber Criminals
- Hacktivist
- Advanced Persistent Threat (APT)
- Nation-State Actor

Certifications ~= Competent

- Offensive Security Certified Professional (OSCP)
- Licensed Penetration Tester (LPT)
- Open Source Security Testing Methodology Manual Professional Security Tester
- Certified Incident Handler (GCIH)
- Certified Ethical Hacker (CEH)
- PenTest+

Testing Methods

- **White Box**
  - Organizational Structure: Full Access
  - Network Architecture: Partial to Full Access
  - Application Testing: Source Code Provided
  - Cost to Test: Least Expensive

Testing Methods

- **White Box**
- **Black Box**
  - Organizational Structure: No Access
  - Network Architecture: No Access
  - Application Testing: No Access
  - Cost to Test: Most Expensive

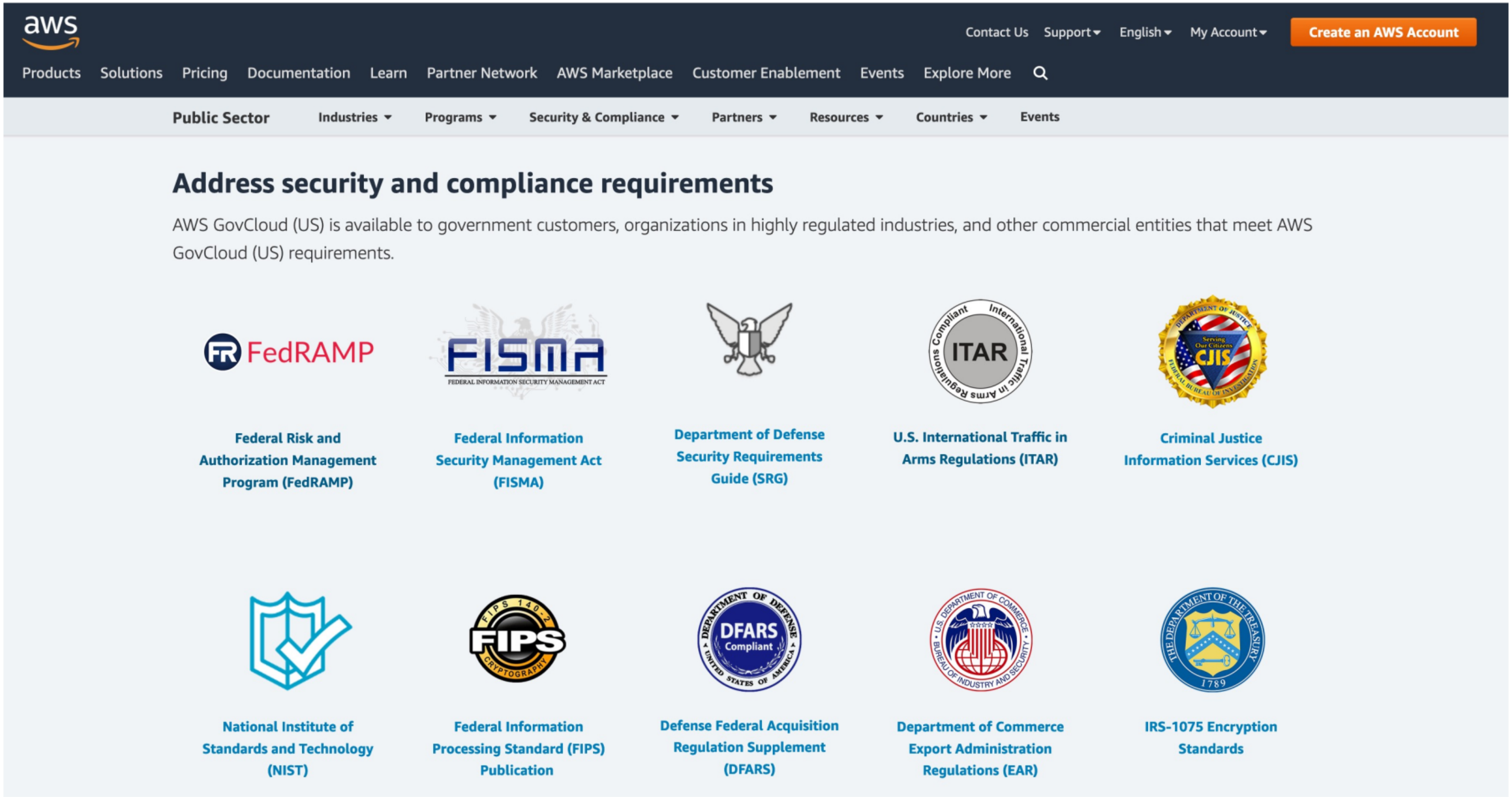
Testing Methods

- **White Box**
- **Black Box**
- **Gray Box**
  - Organizational Structure: Partial Access
  - Network Architecture: No Access to Partial
  - Application Testing: Some Source Code Provided
  - Cost to Test: In Between

Types of Assessments

- **Compliance Test** --- Uses an industry or gov standard as precise requirements
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Federal Information Security Management Act (FISMA)
  - Security Technical Implementation Guides (DISA STIG)

Certified != Secure



Address security and compliance requirements

AWS GovCloud (US) is available to government customers, organizations in highly regulated industries, and other commercial entities that meet AWS GovCloud (US) requirements.

Federal Risk and Authorization Management Program (FedRAMP)

Federal Information Security Management Act (FISMA)

Department of Defense Security Requirements Guide (SRG)

U.S. International Traffic in Arms Regulations (ITAR)

Criminal Justice Information Services (CJIS)

National Institute of Standards and Technology (NIST)

Federal Information Processing Standard (FIPS) Publication

Defense Federal Acquisition Regulation Supplement (DFARS)

Department of Commerce Export Administration Regulations (EAR)

IRS-1075 Encryption Standards

Types of Assessments

- **Compliance Test** --- Uses an industry or gov standard as precise requirements
  Vulnerability Assessment --- Create a consolidated list of specific vulnerabilities within a target environment
  - To identify and help mitigate vulnerabilities in an organization

Types of Assessments

- **Compliance Test** --- Uses an industry or gov standard as precise requirements
  Vulnerability Assessment --- Create a consolidated list of specific vulnerabilities within a target environment
- **Penetration Test** --- Identify vulns and demonstrate exploits against target env

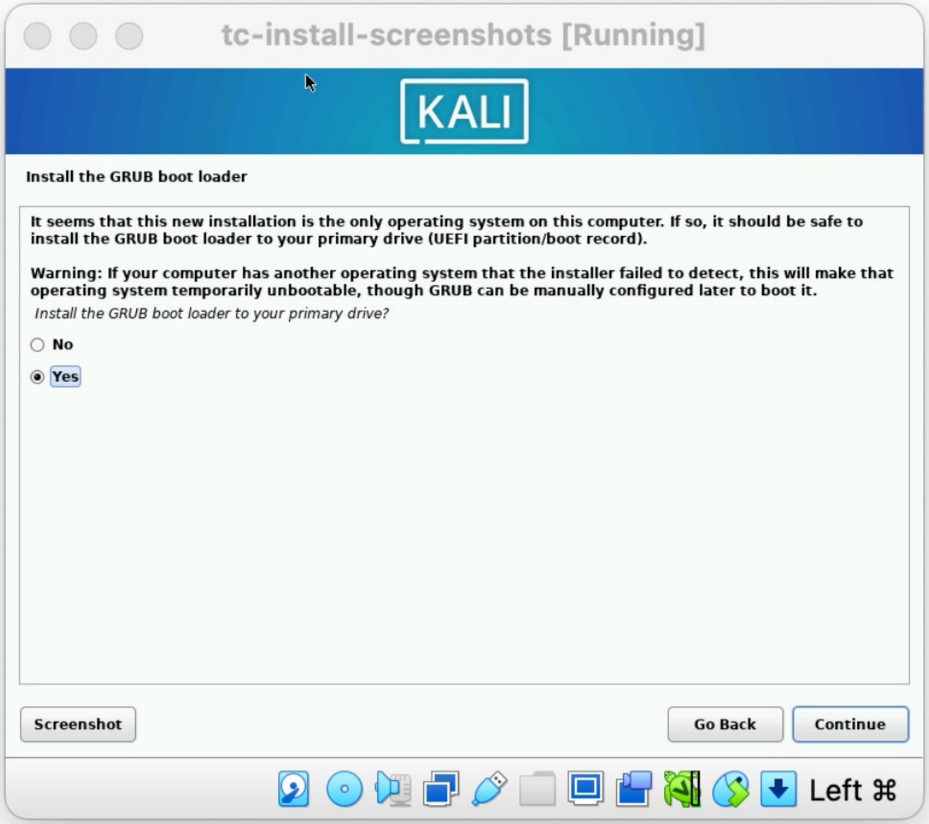
Types of Assessments

- **Compliance Test** --- Uses an industry or gov standard as precise requirements
- **Vulnerability Assessment** --- Create a consolidated list of specific vulnerabilities within a target environment
- **Penetration Test** --- Identify vulns and demonstrate exploits against target env
- **Application Assessment** --- Evaluate desktop, web, or mobile applications to identify insecure code/architecture

Legal Considerations

- **I am not a lawyer which means I am not *YOUR* lawyer. See *YOUR* lawyer for legal advice.**
- DO NOT CONDUCT SECURITY TESTING AGAINST ANY ENTITY UNLESS:
  - The testing activity is legal in the country, state, or city you are testing in
  - You have written authorization by an appropriate decision maker in the organization you are testing against

Installing Kali



Install the GRUB boot loader

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 your primary drive (UEFI partition/boot record).

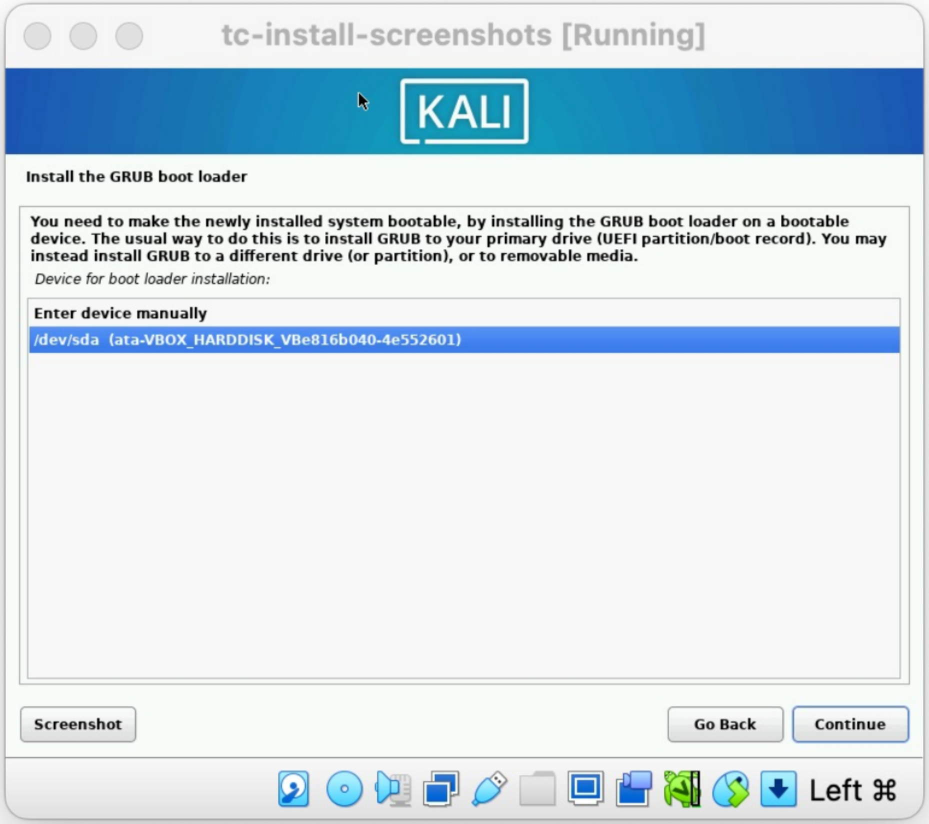
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to your primary drive?

○ No

● Yes

Installing Kali



Install the GRUB boot loader

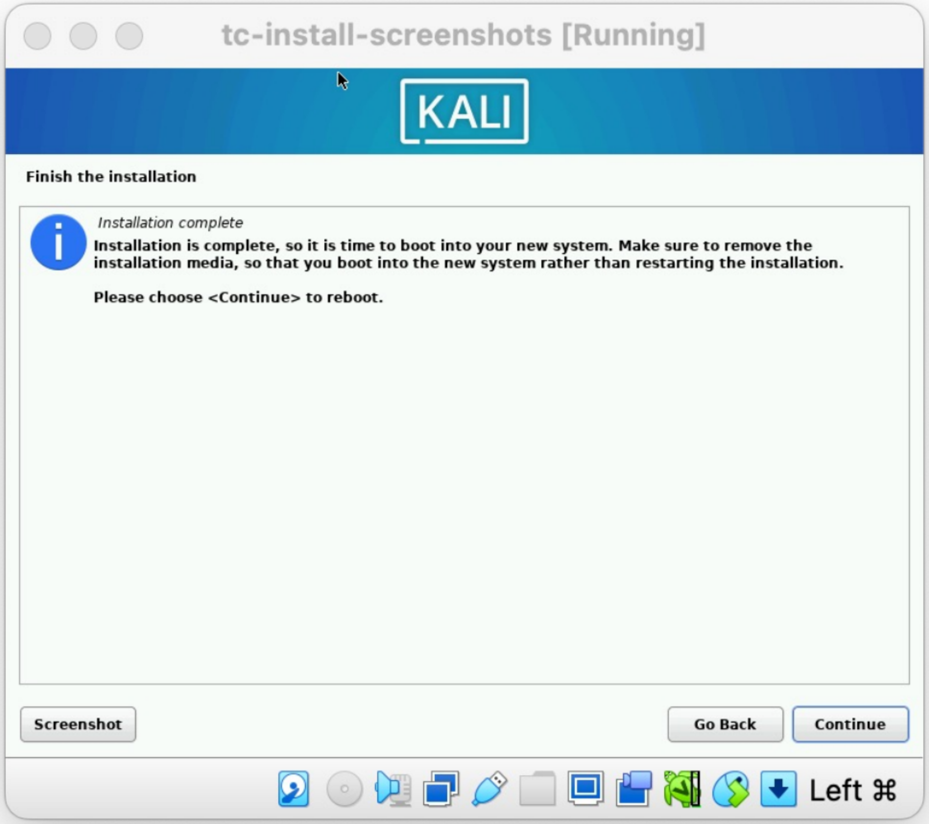
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Enter device manually

/dev/sda (ata-VBOX_HARDDISK_VBe816b040-4e552601)

Installing Kali



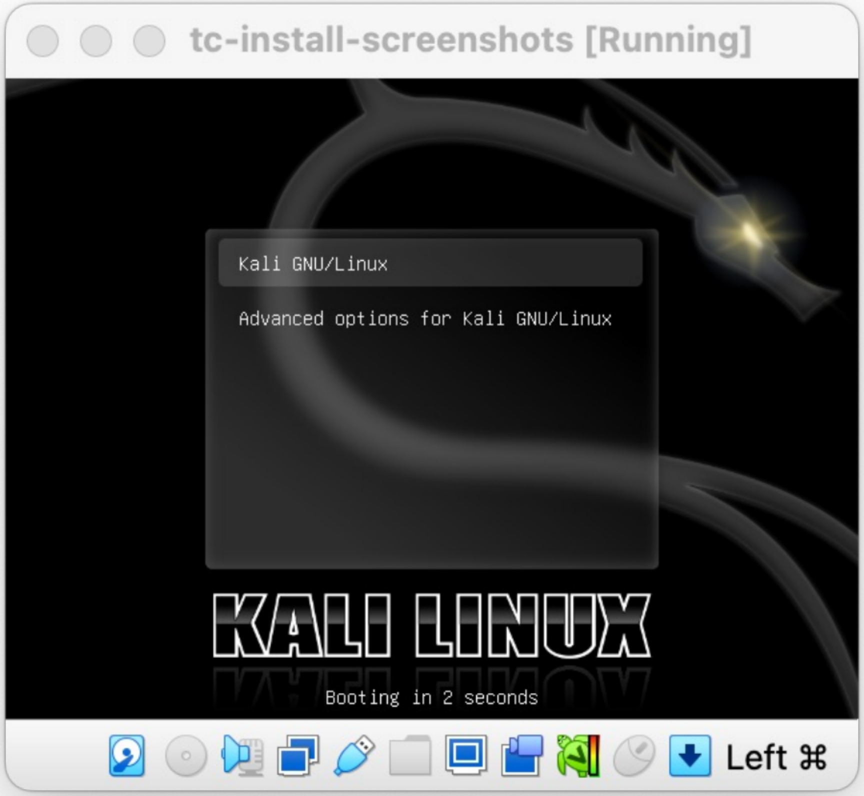
Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.

Installing Kali

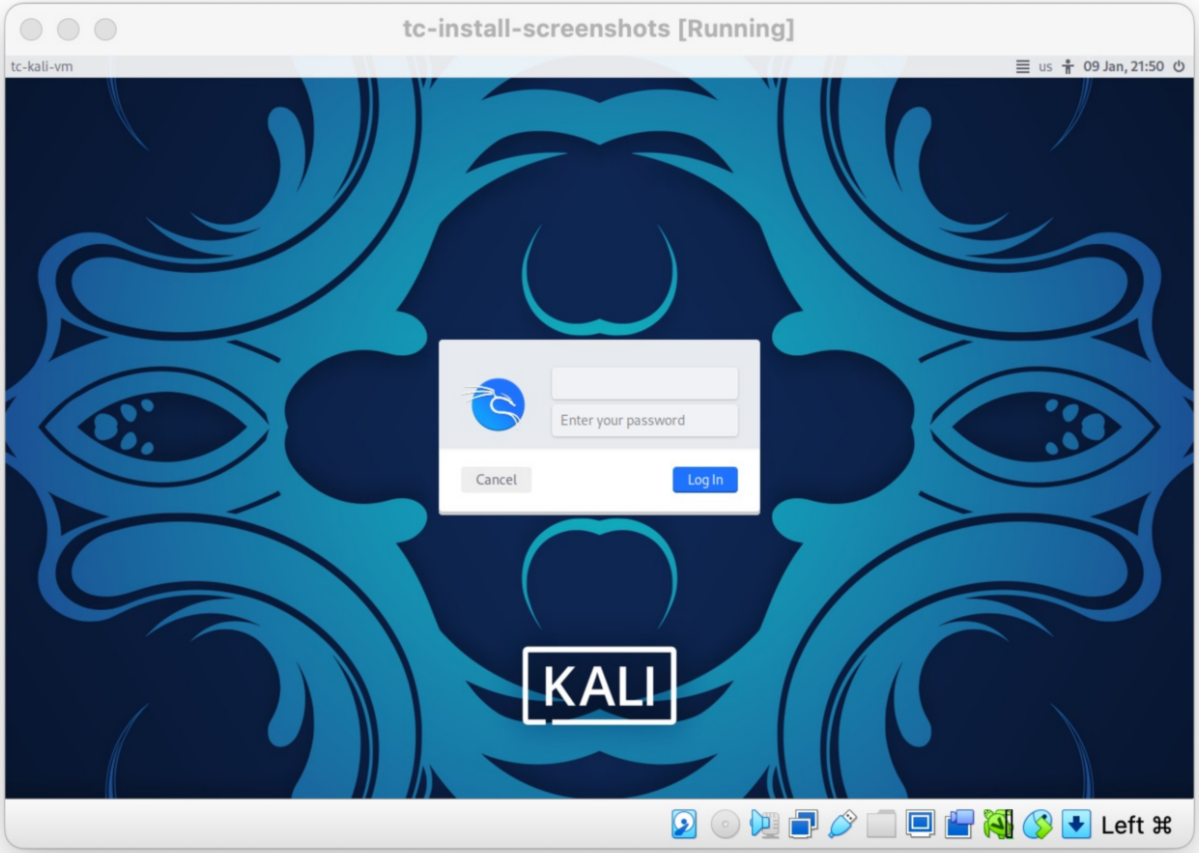


Kali GNU/Linux

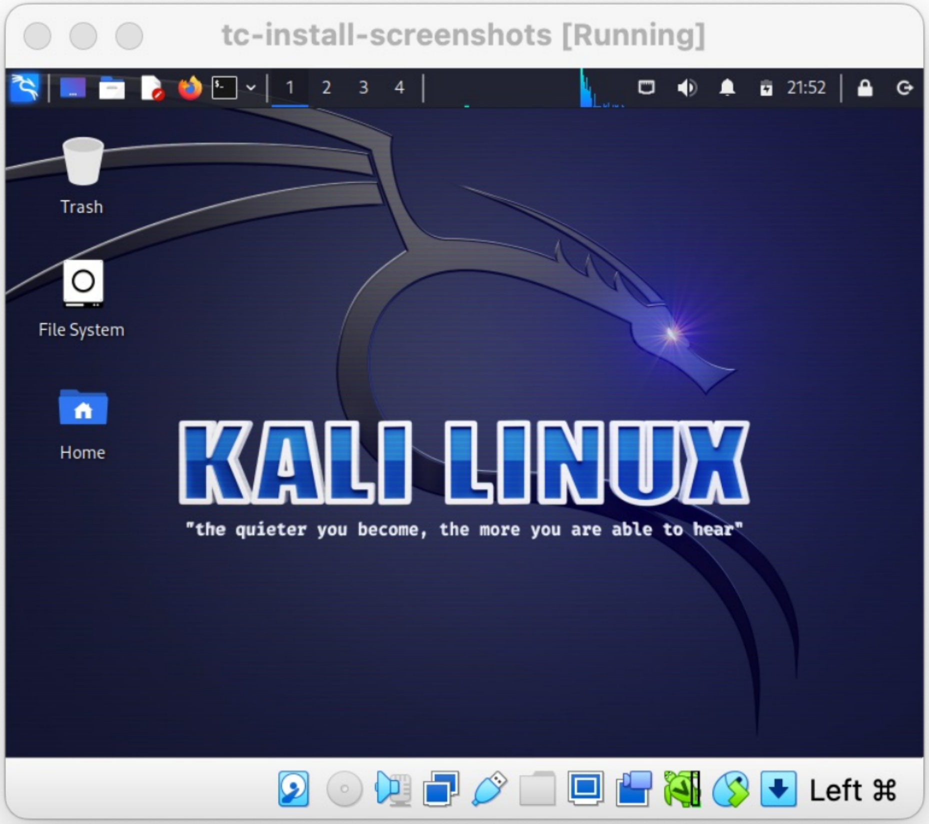
Advanced options for Kali GNU/Linux

Booting in 2 seconds

Installing Kali



Installing Kali


tc-install-screenshots [Running]
1
2
3
4
21:52
Trash
File System
Home
KALI LINUX
"the quieter you become, the more you are able to hear"
Left ⌘