**Tìm hiểu một số công cụ trong Kali Linux ứng dụng trong An ninh mạng**

1. **Giới thiệu tổng quan**
2. **Tổng quan về bảo mật mạng**

* Giới thiệu về bảo mật
* Sự kiện bảo mật năm 2014
* Heartbleed
* Shellshock
* Mã độc mã hóa dữ liệu và tống tiền
* Sony Pictures bị hack

1. **Giới thiệu về các giai đoạn tấn công**

* Thăm dò
* Quét hệ thống
* Chiếm quyền điều khiển
* Duy trì điều khiển hệ thống
* Xóa dấu vết

1. **Các phương thức tấn công mạng**

* Tấn công vào hệ điều hành
* Tấn công ở mức ứng dụng
* Tấn công từ chối dịch vụ
* Tấn công SQL Injection
* Tấn công XSS
* Tấn công vào lỗi cấu hình hệ thống

1. **Tổng quan về Kali Linux**

* Giới thiệu
* Lịch sử
* Đặc điểm phát triển

1. **Tìm hiểu kiến thức**
2. **Giới thiệu về các công cụ trên Kali Linux**

* Thu thập thông tin( Information Gathering)
* Phân tích lỗ hổng( Vulnerability Analysis)
* Ứng dụng web( Web Applications)
* Tấn công mật khẩu( Password Attacks)
* Tấn công mạng không dây( Wireless Attacks)
* Nghe lén/ Giả mạo( Sniffing/ Spoofing)
* Duy trì kết nối( Maintaining Access)
* Kiểm tra hiệu năng( Stress Testing)
* Các công cụ báo cáo( Reporting Tools)

1. **Tìm hiểu về công cụ thu thập thông tin(Nmap)**

* Nguyên tắc truyền thông tin TCP/IP
* Cấu tạo gói tin TCP
* Khi Client muốn thực hiện một kết nối TCP với Server
* Khi Client muốn kết thúc một phiên làm việc với Server
* Nguyên tắc Scan port trong một hệ thống
* TCP Scan
* UDP Scan
* Sử dụng Nmap để Scan port
* Các giai đoạn của Nmap scan
* Các dạng scan mà Nmap hỗ trợ
* Các option kết hợp với các dạng Scan trong Nmap

1. **Tìm hiểu công cụ phân tích lỗ hổng(Nessus)**
2. **Tìm hiểu công cụ crack password**

* Giới thiệu
* Passive online attack
* Active online attack
* Offline attack

1. **Tìm hiểu công cụ đánh giá mức độ an toàn của mạng không dây**

* Giới thiệu
* Bẻ khóa mật khẩu mạng không dây sử dụng mã hóa WEP
* Giao thức WEP
* Hạn chế của WEP
* Thử nghiệm crack khóa WEP
* Giao thức WPA
* Hạn chế của WPA
* Thử nghiệm crack khóa WPA

1. **Cài đặt Kali Linux**
2. **Triển khai các công cụ đánh giá bảo mật trên Kali Linux**

* Triển khai công cụ thu thập thông tin( Nmap)
* Triển khai công cụ phân tích lỗ hổng( Nessus)
* Triển khai công cụ đánh giá mức độ an toàn về giao thức sử dụng trong mạng không dây( WPA)
* Triển khai một giải pháp tăng cường tính bảo mật cho hệ thống
* Ngăn chặn quét port
* Hạn chế lỗ hổng bảo mật
* Đối phó với crack password
* Bảo mật mạng không dây

1. **Đánh giá và hướng phát triển**

* Đánh giá đề tài( Đạt được và hạn chế)
* Hướng phát triển

1. **Tài liệu tham khảo**

<https://123doc.org//document/4003918-do-an-tot-nghiep-danh-gia-bao-mat-he-thong-mang-cong-cu-kali-linux.htm>

<https://whitehat.vn/threads/kali-linux-toan-tap.1120/>

<https://quantrimang.com/cach-cai-dat-va-su-dung-kali-linux-126114>

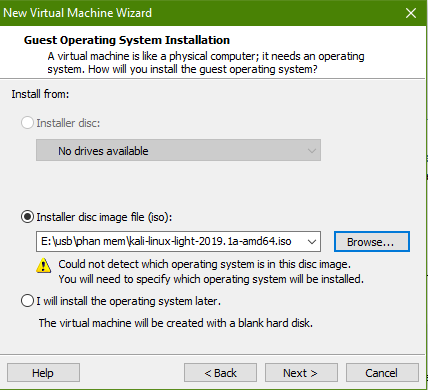
[https://123doc.org//document/1140944-campus-network.htm](https://123doc.org/document/1140944-campus-network.htm?fbclid=IwAR1G1P6tz3aq9EGsowMdXt33kEhxf3UVwk6XeCtxhpYYW-uzngjDsCPJ22M)

* Kali Linux là phiên bản tiến hóa của hệ điều hành BackTrack.
* Xuất hiện vào năm 2013.
* Là hệ điều hành được sử dụng nhiều nhất bởi các chuyên gia đánh giá bảo mật vì nó tích hợp nhiều công cụ chuyên dụng giúp chúng ta đánh giá sự an toàn của một hệ thống.
* Một số đặc điểm nổi bật của Kali Linux:
* Phát triển trên nền tảng hệ điều hành Debian
* Tính tương thích kiến trúc
* Hỗ trợ mạng không dây tốt hơn
* Khả năng tùy biến cao
* Dễ dàng nâng cấp giữa các phiên bản Kali trong tương lai

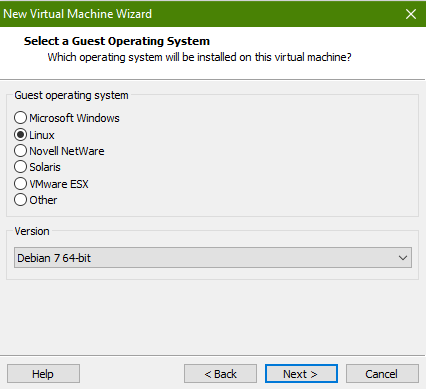
Các bạn mở vmware lên chọn tạo máy ảo



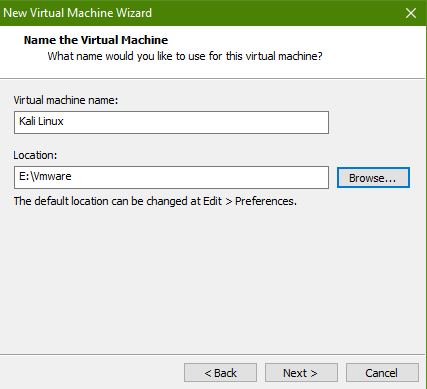
Chọn **typical (recommended)**, sau đó **next**



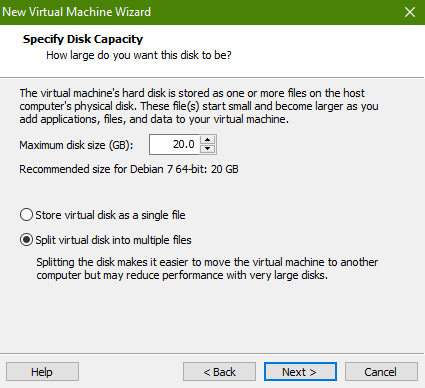
Tick vào dòng **Installer disc image** nhấp vào **browse** để tìm đến file iso kali vừa tải về, sau đó **next**



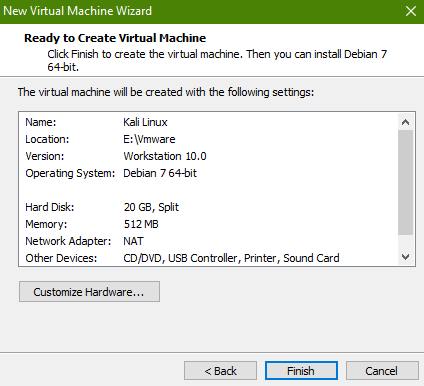
Tiếp theo tick vào ô **Linux**, sau đó xuống dòng **version** chọn **debian 7.x64-bit** (nếu file kali là 64 bit) (nếu các bạn dùng kali-linux 32 bit thì chọn **debian 7.x**)



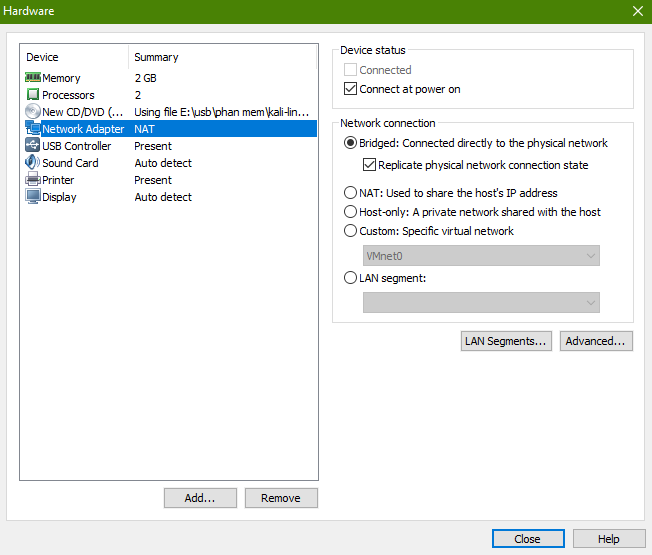
Tiếp theo các bạn đặt tên cho virtual (có thể giữ nguyên không đặt cũng được), sau đó chọn **browse** để tìm đến ổ đĩa để cài ( có thể chọn ổ D, E cũng được), sau đó **next**



Tiếp theo bạn chọn dung lượng của ổ đĩa để cài kali **( nên đặt >40GB)**, sau đó **next**

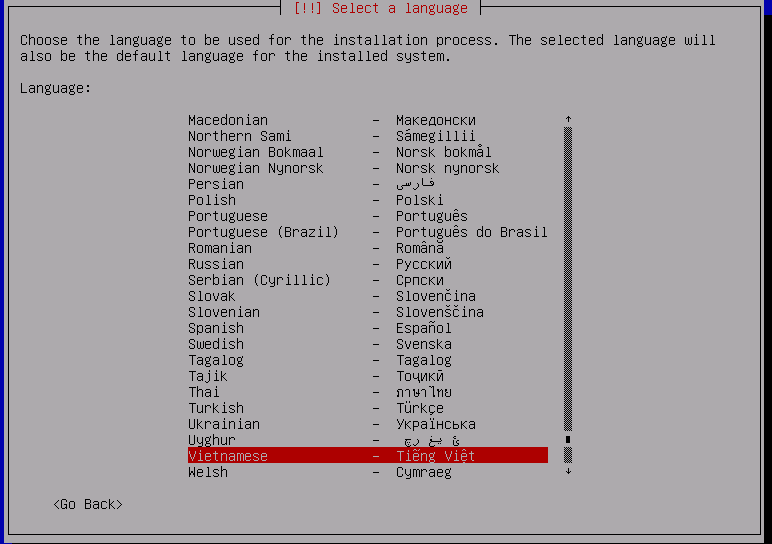


Các bạn chọn **customize hardware** để chỉnh sửa một vài thông số

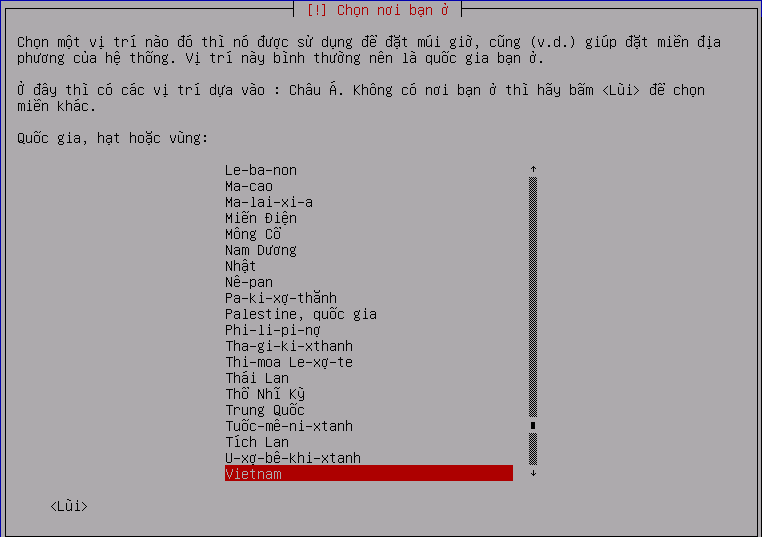


Các bạn chỉnh sửa 3 thông số sau: **Ram >= 1,5GB** - **processors > 2** - **Network chọn bridged**, sau đó **close** để vmware bắt đầu chạy quá trình cài đặt

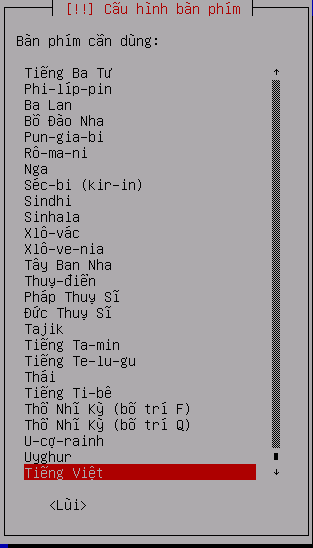
Ở đây có rất nhiều tùy chọn cho các bạn lựa chọn, **Graphical install** (giao diện đồ họa hỗ trợ), **Install** (giao diện dòng lệnh). Ở đây mình chọn **install**



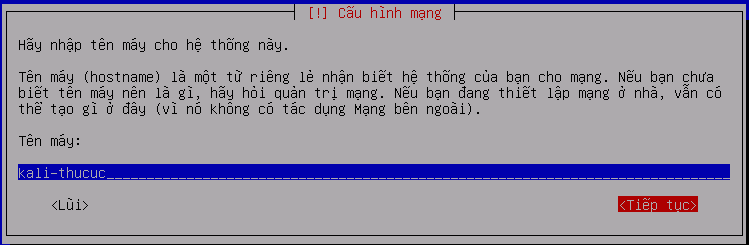
Ở đây các bạn chọn ngôn ngữ cho kali, mình chọn **Tiếng Việt**



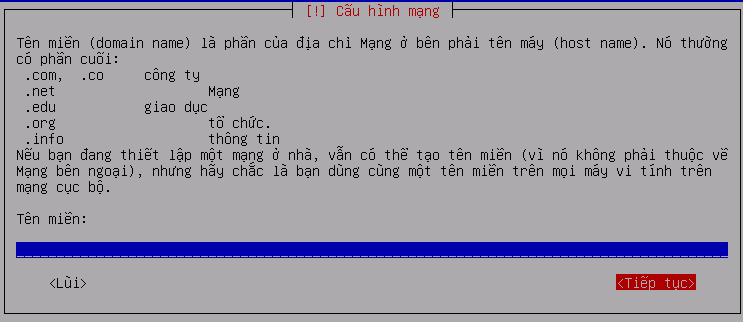
Chọn vị trí địa lí, chọn **Việt Nam**



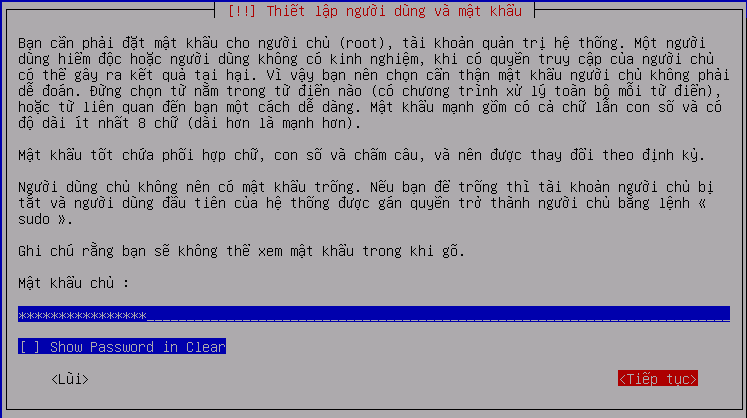
Chọn bộ gõ cho bàn phím, các bạn chọn **Tiếng Việt**



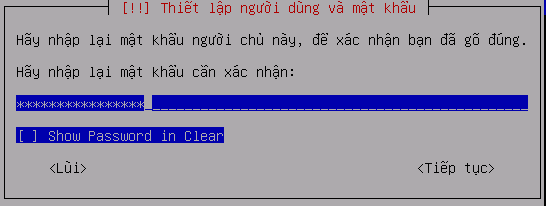
Tiếp theo các bạn đặt tên cho máy ảo, sau đó **tiếp tục**



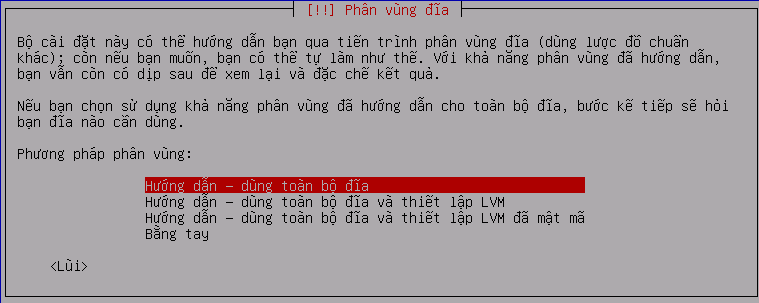
Tiếp tục cấu hình **domain**. Nếu dùng máy theo kiểu cá nhân thì bạn cứ **bỏ qua bước này**, chọn **Tiếp tục** cũng được, hệ thống sẽ tự tạo ra 1 domain với tên gọi **localhost**



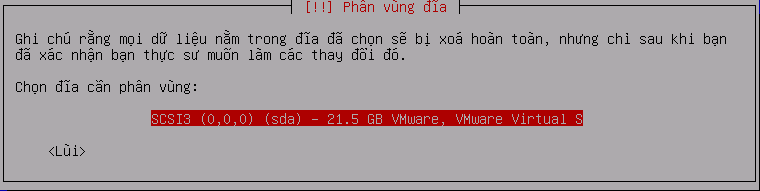
Tiếp theo các bạn đặt **password** cho user của mình (user root -quản trị), sau đó chọn **tiếp tục**



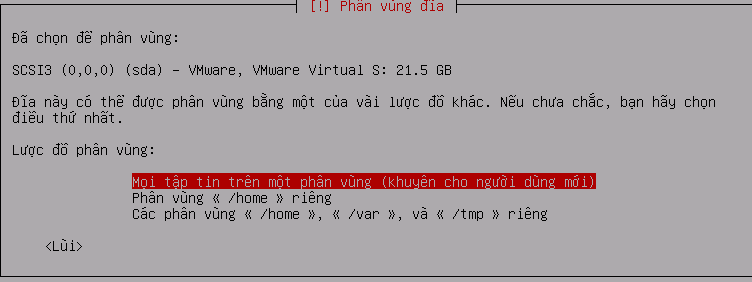
Nhập lại **password** một lần nữa để xác nhận , sau đó chọn **tiếp tục**



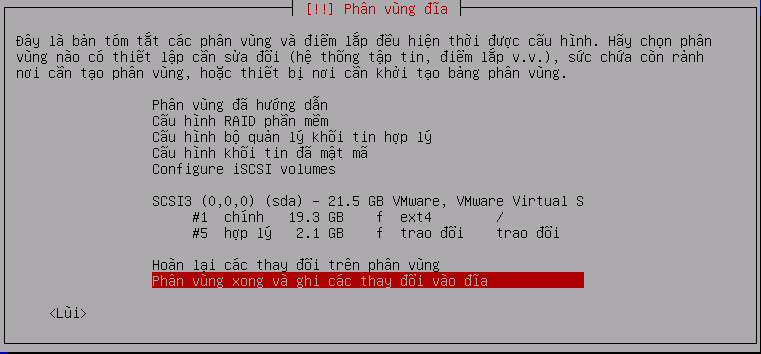
Tiếp theo kali-linux yêu cầu bạn chọn phân vùng định dạng cho ổ cứng và sử dụng phần nào, các bạn chọn **toàn bộ ổ đĩa**



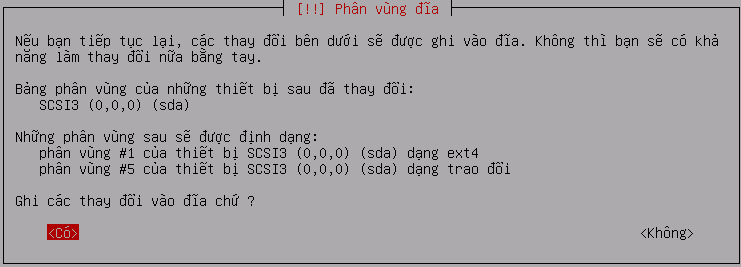
Tiếp theo chọn ổ đĩa mà chúng ta đã thiết lập



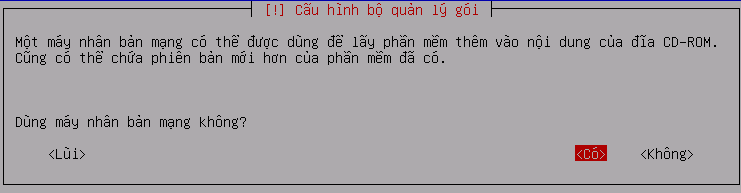
Các bạn chọn **mọi tập tin trên một phân vùng** để đặt tất cả file vào một chỗ



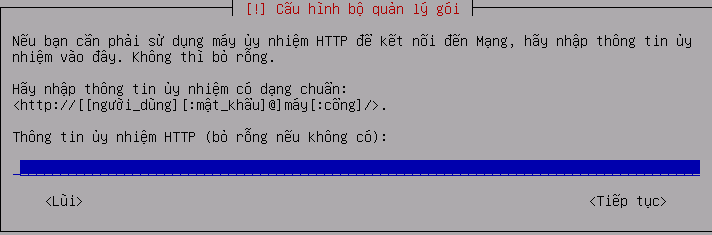
Chọn **phân vùng xong và ghi các thay đổi vào đĩa**



Chọn **có** để lưu thay đổi

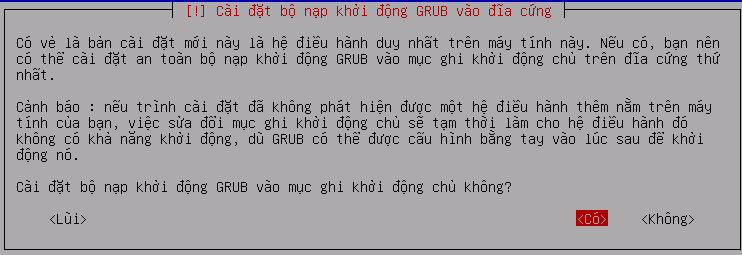


Tiếp theo chọn **có** để dùng bất kì mạng nào để update sau này

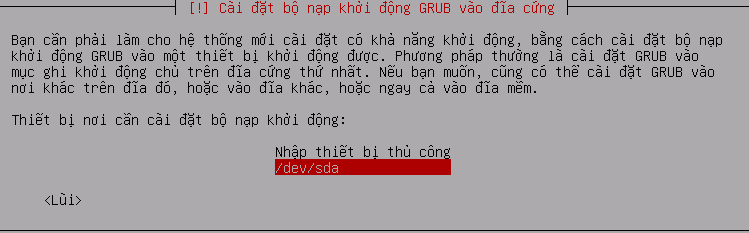


Bỏ qua phần này chọn**tiếp tục**

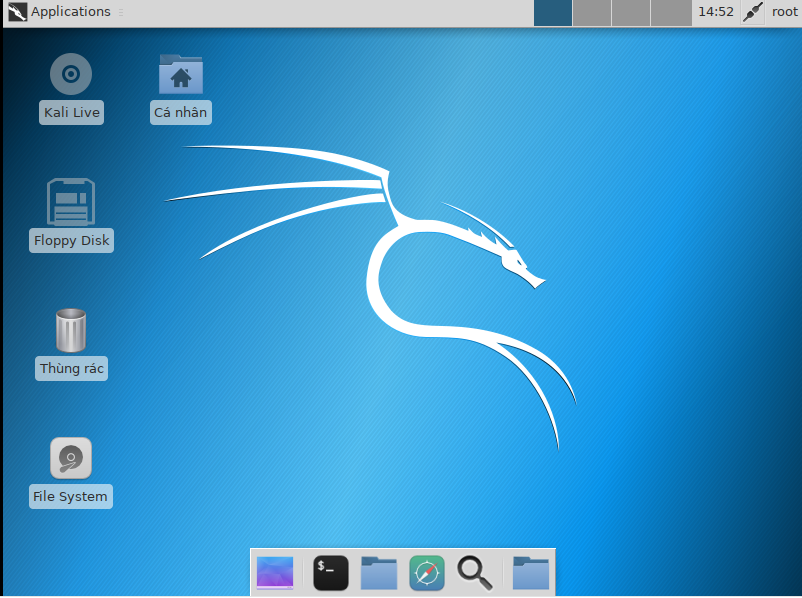
Tại bước này **rất quan trọng** , khởi động được kali hay không là do đây, các bạn phải chắc chắn là chọn **có**



Chọn **/dev/sda** để hệ thống đặt Grub vào đây



Hệ thống sẽ chạy vài phút nữa nếu xuất hiện bản thông báo này là thành công, chọn **tiếp tục** hệ thống sẽ khởi động lại. Tùy mỗi máy có máy sẽ chạy tiếp sau đó mới khởi động lại, có máy thì không khởi động các bạn tự khởi động thủ công



<https://quantrimang.com/nhung-lenh-kali-linux-thuong-dung-147549>

<https://www.mystown.com/2016/03/huong-dan-su-dung-nmap-e-scan-port-tren.html>

<https://anninhmang.edu.vn/nhung-tool-danh-cho-dieu-hanh-kali-linux-nguoi-lam-bao-mat-nen-biet/>

demo

<https://www.giamsatanninhmang.com/2017/04/lab-khai-thac-lo-hong-bao-mat.html>