Getting Started – Bắt Đầu:

1. Linux?

* Từ hệ điều hành Linux, người ta phát triển nhiều phiên bản hệ điều hành khác (Distro), tạo thành các dòng hệ điều hành khác nhau như Debian, Fedora, …
* Kali Linux thuộc dòng Debian

1. Cách Cài Đặt?

* Vào Link
* <https://www.kali.org/get-kali/#kali-platforms>
* Click “Installer Images” + cuộn xuống Click “Installer” + chờ nó tải 4 GB
* Vào Link
* <https://rufus.ie/en/#google_vignette>
* Cuộn xuống Click Link đầu tiên bên dưới “Latest releases” + chờ nó tải + cắm USB 1 vào máy, đảm bảo USB rỗng + chạy chương trình vừa tải + tại mục “Device” chọn cái USB mình vừa cắm + Click nút “SELECT” + chọn File ISO mới tải ở trên + chờ + Click “START” + Tick Option có chữ “DD Image” + Click “OK” + Click “Yes” + chờ nó tải 3 cái File phụ + Click “OK” + chờ nó đốt File ISO vào USB cực lâu + Click “CLOSE” + khi này USB thuộc kiểu CD Drive, nghĩa là bạn sẽ không thấy nó hiện ở File Explorer + phân vùng ổ cứng ra cỡ 80 GB, để nó trống không cần đụng tới hay đặt tên, đây là phân vùng chứa toàn bộ File của Kali Linux, gọi là phân vùng Kali Linux
* Lí do phải sử dụng phần mềm trên thay vì giải nén thẳng File ISO vào USB 1 là vì để USB 1 trở thành thiết bị có thể Boot thì nó phải chứa các File dành cho việc Boot mà khi giải nén không có
* Lấy USB 2 cắm vào máy + vào Link
* <https://git.kernel.org/pub/scm/linux/kernel/git/firmware/linux-firmware.git/>
* Click Link ngay dưới mục “Download” + chờ nó tải File nén toàn bộ Firmware hơn 500 MB + giải nén File này được 1 thư mục, Copy toàn bộ File trong thư mục này thẳng vào USB 2
* Chưa tháo 2 USB vội + khởi động lại máy để vào BIOS + vào Tab “Security” + Double Click “Secure Boot” + Double Click “Secure Boot Support” + Double Click “Disabled” để khi chọn hệ điều hành Kali Linux nó không báo là Virus + chỉnh độ ưu tiên các thiết bị Boot cho thằng USB CD Drive lên đầu + xác nhận các thay đổi và khởi động lại máy + màn hình cài đặt Kali Linux hiện ra, nhấn mũi tên lên xuống để chọn chế độ cài đặt, có thể là chế độ UI xấu hoặc đẹp, nên chọn cái “Graphical install” + tiến hành chọn ngôn ngữ, nước, …, chọn mặc định hết + chờ nó thông báo mình thiếu Firmware + chọn “<Continue>” + chọn Wifi bạn biết mật khẩu + chọn kiểu bảo mật của nó + nhập mật khẩu + chọn <Continue> + nhập tên mà khi kết nối mạng LAN sẽ hiển thị với người khác + nhập tên miền đéo gì cũng được + nhập tên mà khi gửi Email hay gì đó thì hiện lên + nhập tên đăng nhập + nhập mật khẩu đăng nhập + nhập mật khẩu lần 2 + chọn “Eastern” + chọn “use the largest continuous free space”, nghĩa là nơi lưu hệ điều hành sẽ cái phân vùng to vãi lồn chưa bị chiếm mình đã tạo ở trên + chọn “All file in one partition” + chọn “Finish partitioning and write changes to disk” + chọn “<Yes>” + chọn <Continue> 2 lần + chờ nó tải các Tool mặc định + gỡ 2 USB + chọn “<Continue>” để khởi động lại máy + vào BIOS + vào thiết bị Boot là đĩa cứng + chỉnh độ ưu tiên của Kali Linux ứng với “kali” lên đầu + xác nhận và khởi động lại + màn hình chọn hệ điều hành Kali Linux hay Windows hiện ra, gọi là GRUB + chọn cái mong muốn

1. Lỗi No Such Partition Khi Khởi Động?

* Gõ lệnh sau để hiện ra toàn bộ phân vùng ổ cứng trên máy

ls

* Màn hình

(hd0) (hd0,gpt8) …

* Gõ lệnh sau để hiện nội dung trong phân vùng nào đó

ls <Phân Vùng>

* Ví dụ

ls (hd0,gpt8)

* Nếu nó thông báo hệ thống File không xác định thì đây không phải là phân vùng chứa Kali, nếu nó thông báo hệ thống File là ext2 (Second Extended File System), đây là hệ thống File dành cho Kali, do đó đây là phân vùng chứa Kali
* Tiếp theo, gõ đoạn Code sau

set boot=<Phân Vùng Chứa Kali>

set prefix=<Phân Vùng Chứa Kali>/boot/grub

insmod normal

normal

* Ví dụ

set boot=(hd0,gpt4)

set prefix=(hd0,gpt4)/boot/grub

insmod normal

normal

* Khi này Kali sẽ được Boot, và màn hình chọn hệ điều hành Kali hay Windows sẽ hiện ra, chọn Kali
* Sau khi vào Kali, đăng nhập bằng tên đăng nhập và mật khẩu
* Tuy nhiên nếu dừng lại ở đây, thì khi khởi động lại vẫn lỗi, đó là do đoạn lệnh trên chỉ thiết lập giá trị cho các File văn bản cấu hình GRUB , để nội dung trong các File văn bản này được cập nhật cho File “/boot/grub/grub.cfg” là File được chạy khi khởi động, vào Root Terminal gõ lệnh

update-grub

grub-install /dev/sda

1. Cấu Trúc Thư Mục?

* Ngoài các File trong phân vùng Kali Linux, bạn có thể truy cập các File trong phân vùng chứa hệ điều hành Windows
* Để truy cập các File trong phân vùng Kali Linux, Click vào biểu tượng “File System” ở Desktop
* Bên trong đây sẽ có các thư mục sau

boot

* Chứa các File dùng để Boot

etc

* Chứa các File cấu hình

home

* Thư mục tương đương thứ mục “Users” trong Windows, tức là chứa các thư mục con là tên của các người dùng, người dùng này không thể truy cập thư mục của người dùng kia

usr

* Chứa các chương trình được cài đặt

root

* Cần tư cách Root để vào thư mục này, chứa các tập tin như khóa SSH, tệp lưu trữ các gói tin từ các Wifi, …, mặc định tất cả thư mục bên trong nó bị ẩn
* Để truy cập các File trong phân vùng Windows, Click biểu tượng “Windows” ở Desktop và nhập mật khẩu đăng nhập Windows
* Bạn có thể thêm và chỉnh sửa File trong phân vùng Windows, tuy nhiên, các File bạn tạo ra khi đang ở hệ điều hành Linux đều sẽ không có phần mở rộng, nên kiểu gì khi bạn trở lại Windows thì File đó được coi là thuần văn bản
* Các loại File trong Linux

Thuần văn bản, “Plain text document”, biểu tượng tờ giấy có văn bản

File thực thi, “Executable”, biểu tượng bánh răng

1. Desktop?

* Thanh công cụ tồn tại ở bất kì đâu khi bạn vào bất kì chỗ nào, nó nằm ở trên cùng màn hình
* Trên thanh công cụ, bạn sẽ thấy có các biểu tượng đánh số 1, 2, 3, 4, …, đây tượng trưng cho các trang, mỗi trang sẽ mở các chương trình khác nhau, có thể chuyển qua lại giữa các trang bằng cách Click vào biểu tượng số tương ứng

1. Biến Môi Trường?

* Tất cả biến môi trường sẽ lưu trong File “/etc/environment”
* Để chỉ định 1 biến mới làm biến môi trường cho Terminal hiện tại, không có tác dụng với Terminal khác và biến mất khi đóng Terminal

export <Tên Biến>=<Giá Trị>

Terminal:

1. Mở Terminal?

* Mỗi 1 Terminal đang mở sẽ có 2 thuộc tính chính là thư mục làm việc đầu tiên và thư mục làm việc hiện tại
* Nếu thư mục làm việc đầu tiên là “/root” thì bạn có thể dùng lệnh tùy ý, nếu không thì một số lệnh sẽ bị hạn chế, khi này gọi là Root Terminal
* Để mở nhanh 1 Terminal với thư mục làm việc ban đầu là “/root”, Click biểu tượng Root Terminal Emulator trên thanh công cụ, còn muốn thư mục làm việc ban đầu là

“/home/<Tên Người Dùng Hiện Tại>” thì Click biểu tượng Terminal Emulator trên thanh công cụ hoặc nhấn “Ctrl” + “Alt” + “T”

* Nếu thư mục làm việc đầu tiên đang là “/root”, thì đầu mỗi câu lệnh sẽ có chuỗi

“rootⓀ<Tên Miền>”, còn nếu là “/home/<Tên Người Dùng Hiện Tại>” thì sẽ có chuỗi

“<Tên Người Dùng Hiện Tại>Ⓚ<Tên Miền>”, ngoài ra bên phải chuỗi này còn hiện thư mục làm việc hiện tại, kí hiệu ~ tượng trưng cho thư mục làm việc đầu tiên

* Để chuyển thư mục làm việc đầu tiên thành “/root”, nhập lệnh

sudo su

* Khi đứng trong 1 thư mục, phải chuột + chọn “Open Terminal Here”, 1 Terminal mới sẽ được mở, với thư mục làm việc đầu tiên là “/home/<Tên Người Dùng Hiện Tại>” và thư mục làm việc hiện tại là thư mục mình đang đứng tại

1. Trả Về Đường Dẫn Tuyệt Đối Của Thư Mục Làm Việc Hiện Tại?

pwd

1. Hủy Lệnh Đang Nhập Dở Dang?

* Nhấn “Ctrl” + “C”

1. Thay Đổi Thư Mục Làm Việc Hiện Tại?

* Để từ thư mục cha xuống thư mục con trực tiếp

cd <Tên Thư Mục Con>

* Ví dụ

cd foo

* Để từ thư mục hiện tại nhảy lên thư mục cha

cd ..

* Để thay đổi thư mục làm việc hiện tại thành thư mục làm việc đầu tiên

cd ~

* Để kết hợp nhiều lệnh cd, đặt dấu / ở giữa
* Ví dụ

cd ../../etc/foo

* Tương đương

cd ..

cd ..

cd etc

cd foo

Internet – Mạng:

1. Mạng?

* Khi cài Kali Linux tự động có Firefox
* Để xem tên Card mạng và Wifi đang kết nối, vào Terminal, nhập

iwconfig

* Tên Card mạng sẽ ở cột bên trái, thông tin ở cột bên phải
* Để chuyển Card mạng sang chế độ Monitor

airmon-ng start <Tên Card Mạng>

* Ví dụ

airmon-ng start wlan0

* Khi chuyển sang chế độ này rồi thì Card mạng sẽ ngắt kết nối với Wifi hiện tại đang kết nối nếu nó đang ở chế độ Managed, đồng thời kể từ đây bạn không thể kết nối với Wifi nào được nữa, tên Card mạng cũng bị đổi, gọi là tên Card mạng Monitor, ví dụ từ wlan0 thành wlan0mon
* Để bắt lắng nghe tất cả các sóng Wifi xung quanh

airodump-ng <Tên Card Mạng Monitor>

* Ví dụ

airodump-ng wlan0mon

* Khi này Terminal sẽ bắt đầu hiển thị thông tin các sóng Wifi xung quanh, gồm tên Wifi, BSSID của nó, …, để tắt chế độ này, nhấn “Ctrl” + “C”
* Để chỉ lắng nghe 1 sóng Wifi nào đó, thêm cờ sau

–bssid <BSSID Của Wifi>

* Ví dụ

airodump-ng –bssid AA:BB:CC:11:22:33 wlan0mon

* Để ghi lại các gói tin đã lắng nghe, thêm cờ sau

–w <Tên File Lưu Trữ>

* Ví dụ

airodump-ng -w foo –bssid AA:BB:CC:11:22:33 wlan0mon

* Khi này, trong thư mục “/root” sẽ xuất hiện 5 File có tên với cú pháp là

“<Tên File Lưu Trữ>-<Index>.<Phần Mở Rộng>”

* Trong đó <Index> là số có 2 chữ số, nếu trong “/root” chưa có File nào với cú pháp này, thì <Index> = 01, nếu đã có, thì <Index> sẽ tăng dần, và lấp chỗ trống nếu có, ví dụ trong “/root” đã có “<Tên File Lưu Trữ>-01” và

“<Tên File Lưu Trữ>-03”, thì <Index> = 02

* <Phần Mở Rộng> tương ứng với 5 File lần lượt là “cap”, “csv”, “kismet.csv”, “kismet.netxml”, “log.csv”
* Để kết thúc lắng nghe, nhấn “Ctrl” + “C”, 5 File kia vẫn tồn tại trên máy, lưu lại các gói tin bắt được từ Wifi mục tiêu, kể cả các gói tin mật khẩu từ sự kiện Handshake

File System – Hệ Thống File:

1. Liệt Kê Tất Cả Thông Tin Của Tất Cả Phân Vùng Trên Máy?

* Vào Terminal, nhập

fdisk -l

1. Hiện Nội Dung Trong 1 File Vào Terminal?

* Vào Terminal, nhập

cat <Đường Dẫn Tới File>

* Ví dụ

cat /home/foo

1. Hiện File Bị Ẩn?

* Nhấn “Ctrl” + “H” để chuyển đổi qua lại giữa hiện File bị ẩn và ẩn File bị ẩn

1. Tìm 1 File?

find <Đường Dẫn> -name <Tên File>

* Lệnh trên sẽ hiển thị đường dẫn tuyệt đối của tất cả các File có tên là <Tên File> từ <Đường Dẫn> trở đi
* Ví dụ

find /usr -name foo

* Lệnh trên sẽ hiển thị đường dẫn của tất cả Flle có tên foo nằm trong thư mục “/usr”, không cần là File con trực tiếp

1. Liệt Kê Tất Những Gì Bên Trong 1 Thư Mục?

* Vào Terminal nhập

ls

* Lệnh này sẽ liệt kê tất cả các File và thư mục con trực tiếp trong thư mục làm việc hiện tại
* Liệt kê dưới dạng bảng, thứ tự đọc là đọc hết cột này rồi mới đến cột bên phải, đọc cột từ trên xuống dưới, thứ tự sắp dựa trên tên của File và thư mục, sắp y chang từ điển
* Tên File thì màu trắng, tên thư mục thì màu xanh

User – Người Dùng:

1. Hiện Thông Tin Người Dùng Hiện Tại?

* Vào Terminal, nhập

who

1. Thêm Người Dùng?

* Vào Terminal, nhập

adduser <Tên Người Mới>

* Sau đó nhập mật khẩu mới và 1 số thông tin cá nhân khác

1. Xóa Người Dùng?

* Vào Terminal, nhập

deluser <Tên Người Dùng>

1. Hiện Thông Tin ID Người Dùng?

* Vào Terminal, nhập

id <Tên Người Dùng>

Text Editor – Trình Soạn Thảo:

1. Trình Soạn Thảo Mặc Định?

* Là Mousepad, khi mở 1 File để chỉnh sửa nó sẽ tự động vào Mousepad
* Có thể mở 1 File bằng Mousepad thông qua Terminal

mousepad <Đường Dẫn Tới File Không Có Phần Mở Rộng>

GRUB:

1. Cập Nhật Những Thay Đổi Trong Các File Cấu Hình GRUB?

* Để nội dung văn bản trong các File cấu hình này chuyển thành dạng nhị phân trong File “/boot/grub/grub.cfg”, là File được chạy khi khởi động máy, vào Terminal nhập

update-grub

1. Thay Đổi Hệ Điều Hành Được Boot Mặc Định Và Thời Gian Chờ Để Chọn Hệ Điều Hành?

* Mặc định khi khởi động, bạn sẽ vào màn hình chọn hệ điều hành GRUB, khi này nếu bạn không nhấn phím lên xuống thì sau 5 giây nó sẽ tự động chọn hệ điều hành mặc định, thời gian đếm ngược 5 giây được hiển thị ở bên dưới màn hình, nếu bạn ấn phím lên xuống, thì thời gian đếm ngược sẽ bị vô hiệu hóa
* Để thay đổi hệ điều hành mặc định và thời gian 5 giây, vào File “/etc/default/grub” + chỉnh thuộc tính “GRUB\_DEFAULT” thành Index của hệ điều hành, ví dụ trong màn hình GRUB thứ tự từ trên xuống là A, B, C, …, thì hệ A có Index 0, B có Index 1, … + chỉnh thuộc tính “GRUB\_TIMEOUT” từ 5 thành số giây đếm ngược mong muốn

Package – Gói:

1. Package?

* Các Package được lưu trong thư mục “/usr/bin”
* Để tải 1 Package về máy, dùng apt, nếu không tải được bằng apt thì dùng

apt-get

apt install <Tên Package>

* Để tải những thông tin cần thiết để cập nhận các Package

apt update

* Để thực sự cập nhật các Package dựa vào các thông tin trên

apt upgrade

* Tương tự như trên, nhưng thông minh hơn trong việc xử lí các gói liên quan nhau

apt dist-upgrade

1. Gõ Tiếng Việt?

* Ibus (Intelligent Input Bus) là phần mềm hỗ trợ các phương thức nhập liệu
* Để mở nó và cho nó chạy nền, vào phần ứng dụng bằng cách Click biểu tượng ở sát góc trái trên + nhập “Ibus Preferences” + nhấn “Yes” + nhấn “OK” + vào Tab “Input Method” + tại đây sẽ hiện những bộ gõ trong danh sách bộ gõ hiện tại + để thêm 1 bộ gõ Click “Add” + chọn ngôn ngữ, Click dấu 3 chấm để xem tiếp + chọn 1 trong số các bộ gõ của ngôn ngữ này + Click “Add” + để xóa bộ gõ khỏi danh sách thì Click nó rồi Click “Remove” + để đóng phần mềm Click “Close”
* Khi chạy nền, sẽ có biểu tượng chữ i, vi, …, tùy thuộc vào bộ gõ xuất hiện ở thanh trên cùng bên phải, Click vào biểu tượng này để chuyển đổi qua lại giữa các bộ gõ trong danh sách bộ gõ hiện tại
* Để ngừng chạy nền, phải chuột vào biểu tượng đó rồi Click “Quit”
* Để thêm Option bộ gõ Telex vào ngôn ngữ “Vietnamese”
* Vào Terminal, nhập lệnh sau để tải

apt-get install ibus-unikey

* Khi này bộ gõ có tên “Unikey” sẽ xuất hiện trong phần ngôn ngữ “Vietnamese” để bạn lựa chọn nếu muốn gõ Telex