Unit – Đơn Vị:

1. Băng Thông (Bandwidth)?

* Tốc độ truyền tải dữ liệu
* Có đơn vị cơ bản là bps (Bits Per Second)
* Ví dụ
* 10 bps tương đương truyền được 10 Bit dữ liệu mỗi giây
* 5 Mbps tương đương truyền được 5 Mega Bit dữ liệu mỗi giây

1. Octet?

* = 1 Byte

Protocol – Giao Thức:

1. Giao Thức Thực Chất Là Gì?

* Là 1 dãy các quy tắc phải tuân theo khi 2 thứ giao tiếp với nhau để cuộc giao tiếp được diễn ra thành công
* Các quy tắc của 1 giao thức như quy tắc mã hóa, quy tắc đồng bộ, quy tắc kiểm soát lỗi, …, mỗi giao thức sẽ có 1 bộ quy tắc khác nhau

1. IP (Internet Protocol) Bao Gồm Những Quy Tắc Gì?

* Quy tắc định dạng địa chỉ IP
* Quy tắc phân đoạn dữ liệu
* Quy tắc định tuyến
* Quy tắc kiểm soát lỗi
* …

1. Địa Chỉ IP Công Cộng?

* Là 1 dãy số độc nhất gán cho mỗi thiết bị kết nối trực tiếp vào mạng Internet
* Địa chỉ IP do nhà mạng cung cấp cho bạn là địa chỉ IP công cộng, được gán cho Modem vì nó nối trực tiếp với cái ổ mà nhà mạng cung cấp cho bạn

1. IPv4?

* Loại địa chỉ IP phổ biến nhất hiện tại, có tối đa khoảng 4.3 tỉ địa chỉ loại này, nhưng đã cạn kiệt nên dần được thay thế bởi IPv6
* Được biểu diễn = 1 dãy số thập phân được chia ra thành 4 phần bởi dấu “.”, mỗi phần có giá trị từ 0 đến 255, mỗi phần còn được gọi là 1 Octet vì chứa 8 Bit
* Mỗi dãy số địa chỉ lại được chia thành 2 phần, phần đầu là Network, phần sau là Host đại diện cho thiết bị, vì để quản lý các thiết bị một cách thuận tiện nhất, dùng phương pháp chia để trị, mạng Internet được chia thành các Network, và trong mỗi Network lại bao gồm nhiều Host, để biết được đâu là phần địa chỉ Network, dựa vào 1 dãy số khác luôn đi đôi với địa chỉ IPv4, là Subnet Mask, là dãy Bit có độ dài = địa chỉ IP, lấy Subnet Mask nhân cho địa chỉ IP, được địa chỉ Network, phần còn lại là địa chỉ Host
* Ví dụ
* 1 thiết bị kết nối Internet có địa chỉ IP là 193.123.68.1 và Subnet Mask là 255.255.255.0 thì địa chỉ Network là 193.123.68.0 và địa chỉ Host trong Network là .1

1. Lớp Network?

* Địa chỉ Network của IPv4 lại được chia thành 5 lớp A, B, C, D, E
* Lưu ý mỗi Network sẽ dành ra 2 địa chỉ đầu và cuối làm địa chỉ Network và địa chỉ Broadcast
* Tưởng tượng địa chỉ Network là địa chỉ khu phố, địa chỉ Broadcast là cái loa phát thanh toàn khu phố, các địa chỉ còn lại là số nhá
* Mỗi lớp Network sẽ dành ra 1 phần nhỏ để làm địa chỉ cục bộ
* Lớp A có giá trị từ 1.0.0.0 đến 127.0.0.0 với Subnet Mask 255.0.0.0, tổng cộng 126 Network với tối đa 16777214 Host mỗi Network
* Địa chỉ đặc biệt có giá trị từ 127.0.0.1 đến 127.255.255.255 còn được gọi là địa chỉ Loopback, gọi như vậy vì những địa chỉ dành ra để làm Local Host, tức là bạn gửi yêu cầu đến những địa chỉ này đồng nghĩa gửi yêu cầu với chính máy tính của bạn, riêng 127.0.0.1 sẽ tương ứng với tên miền “localhost”
* Lớp B có giá trị từ 128.0.0.0 đến 191.255.0.0 với Subnet Mask 255.255.0.0, tổng cộng 16382 Network với tối đa 65534 Host mỗi Network
* Lớp C có giá trị từ 192.0.0.0 đến 223.255.255.0 với Subnet Mask 255.255.255.0, tổng cộng 2097150 Network với tối đa 254 Host mỗi Network
* Lớp D có giá trị từ 224.0.0.0 đến 239.255.255.255, dùng để Multicast
* Lớp E có giá trị từ 240.0.0.0 đến 255.255.255.255, dùng để nghiên cứu

1. Địa Chỉ IP Cục Bộ?

* Là địa chỉ thường thấy trên các thiết bị, được lấy ra từ 1 phần nhỏ của mỗi lớp Network
* Những địa chỉ IP này không tồn tại trên Internet, khi đăng kí dịch vụ Internet, nhà mạng sẽ cung cấp cho 1 địa chỉ công cộng, đây mới là địa chỉ của ta trên Internet, là địa chỉ của cái Modem nối trực tiếp với mạng, trong địa chỉ này, tưởng tượng ta lại có cả 1 Internet con nữa bị ẩn khỏi thế giới bên ngoài bao gồm các thiết bị kết nối sau Modem, cấu trúc tương tự như Internet bên ngoài
* Các địa chỉ này có Subnet Mask của lớp tương ứng
* Các địa chỉ này có thể lặp đi lặp lại bởi những người dùng khác nhau, tiết kiệm đáng kể địa chỉ IPv4
* Lớp A có giá trị từ 10.0.0.0 đến 10.255.255.255
* Lớp B có giá trị từ 172.16.0.0 đến 172.31.255.255
* Lớp C có giá trị từ 192.168.0.0 đến 192.168.255.255

1. IPv6?

* Loại địa chỉ IP đang dần được đưa vào sử dụng thay thế cho IPv4, có tối đa khoảng 340 tỉ tỉ tỉ tỉ địa chỉ loại này

1. Xem Địa Chỉ IP Công Cộng Của Mình?

* <https://www.whatismyip.com/>
* Địa chỉ công cộng của bạn nằm ở nhà mạng

1. Địa Chỉ IP Tĩnh Và Động?

* Ví dụ 1 cục Modem khi rút ra ổ mạng rồi cắm lại, địa chỉ IP của nó không thay đổi, thì đây là địa chỉ IP tĩnh, còn nếu nó thay đổi thì là động
* Địa chỉ tĩnh gán cho các thiết bị quan trọng như Server
* Địa chỉ động để kẻ gian khó tấn công

1. Tại Sao Không Sử Dụng IPv6 Cho Tất Cả Thiết Bị?

* Vì đã quen với IPv4, việc thay đổi sẽ rất tốn kém và cần phải diễn ra từ từ

1. Địa Chỉ MAC (Media Access Control)?

* Là địa chỉ gắn với Card mạng trong máy tính, điện thoại, … là dãy số độc nhất cho mỗi Card mạng và không thay đổi cho đến hết đời, còn gọi là địa chỉ vật lý
* Giúp xác định nhà sản xuất
* Gồm 6 Octet, mỗi Octet viết dưới hệ Hexa
* Còn gọi là BSSID (Basic Service Set Identifier) trong trường hợp Card mạng đang ở chế độ Master hay nó đang là Access Point

1. Port?

* Giả sử bạn nhập 1 tên miền nào đó lên trình duyệt và nhấn Enter, nó sẽ được chuyển về địa chỉ IP và máy tính sẽ gửi yêu cầu của bạn đến Server có địa chỉ IP đó, nhưng Server này không chỉ trả về trang Web, mà còn có thể trao đổi File, Email, … vậy thì làm sao nó biết chúng ta muốn sử dụng dịch vụ nào, khi đó mỗi dịch vụ trên Server sẽ được gán cho 1 con số gọi là Port, ví dụ Port 80 trên Server này tương ứng với dịch vụ Web, Port 21 ứng với nơi dịch vụ trao đổi File, …, khi ta gửi yêu cầu đến Server thì địa chỉ IP của Server sẽ được gắn thêm Port ứng với phần đằng trước tên miền, ví dụ “http” thì ứng với Port 80, “ftp” ứng với Port 21, đồng thời trên máy tính của ta cũng xuất hiện 1 Port với 1 con số ngẫu nhiên, ví dụ 49253, số này cũng sẽ được gửi đi cùng với yêu cầu, khi Server nhận được yêu cầu cùng với Port tương ứng, nó sẽ cung cấp dịch vụ dựa theo số Port đó và gửi dữ liệu lại cho máy tính của bạn kèm theo cái số 49253, sau khi máy tính nhận được dữ liệu nó sẽ đưa dữ liệu vào cái Port 49253, mà ở đây có thể là trinh duyệt Web của bạn
* Ví dụ, ta muốn sử dụng dịch vụ Web của Server có tên miền “foo.com” thì nhập “http://foo.com” hoặc “foo.com:80” hoặc “0.1.2.3:80”, 0.1.2.3 là địa chỉ IP ứng với “foo.com”

1. Các Loại Port?

* Từ 0 đến 1023 là các Port thường thấy, ví dụ
* “https” ứng với 443
* “http” ứng với 80
* Từ 1024 đến 49151 là các Port có thể được đăng ký
* Từ 49152 đến 65535 là các Port ngẫu nhiên được sinh ra khi ta trao đổi dữ liệu trên Internet

1. URI, URL, URN?

* Ví dụ có 1 tài nguyên trên mạng là 1 File Word, bạn muốn truy cập File này, nhưng bạn cần biết nó nằm ở đâu, hay tên định danh của nó là gì, khi này URL chính là địa chỉ và URN chính là tên định danh của nó, bạn có thể truy cập File này sử dụng URL hoặc URN, nếu bạn muốn sử dụng cả 2 phương thức thì dùng URI
* URL và URN đều là các dạng của URI
* URL là cái dòng chữ trên thanh tìm kiếm, bao gồm phần đầu là giao thức, ví dụ “http”, phần sau là tên miền, tiếp theo sẽ là số Port hoặc không có số Port, cuối cùng là đường dẫn đến tài nguyên trên Server
* Ví dụ

http://foo.com/bar/foobar.html

* Giả sử bạn thay đổi địa chỉ của File “foobar.html” sang thư mục foo, khi đó URL sẽ đổi thành

http://foo.com/foo/foobar.html

* Tuy nhiên, URN của File “foobar.html” vẫn giữ nguyên

1. Giao Thức Truy Cập Tệp (File Protocol)?

* Giao thức này bắt đầu = “file://”
* Ví dụ
* Khi bạn nhập “file:///C:/Bar/foo.txt” lên trình duyệt thì nó sẽ hiển thị nội dung File có đường dẫn “/C:/Bar/foo.txt” trong máy tính của bạn lên trình duyệt, dấu “/” đằng trước “C” đại diện cho thư mục gốc của máy tính

Device – Thiết Bị:

1. Cáp Đồng Trục (Coaxial Cable)?

* Dây cáp có lõi = đồng, tiếp theo là lớp cách điện, tiếp theo là lớp chống nhiễu = lưới bện đồng, ngoài cùng là nhựa PVC
* Đồng trục là vì các lớp cùng có 1 trục hình học chung
* Đầu cắm dạng hình trụ

1. Cáp Quang?

* Dây cáp có lõi là nhựa thủy tinh bọc lớp phản quang, tiếp theo là lớp cách điện, tiếp theo là lớp chống nhiễu và cuối cùng là lớp nhựa cao su
* Đầu cắm dạng hình trụ
* Tia sáng phản chiếu qua lại trong cáp quang chỉ có biên sóng là A và B tương ứng 0 và 1

1. Cáp Xoắn Đôi (UTP)?

* Dây cáp có 4 cặp dây, mỗi dây đồng được bọc lớp cách điện, mỗi cặp thì lại xoắn lại như DNA và có màu khác nhau, bên ngoài là vỏ bọc chung
* Xoắn lại để chống nhiễu thông tin
* Đầu cắm dạng hình hộp chữ nhật

1. Ethernet?

* Là 1 công nghệ mạng giúp truyền dữ liệu giữa các thiết bị trong mạng LAN
* Giao thức Ethernet bao gồm
* Quy tắc kết nối giữa các thiết bị = cáp đồng trục, cáp quang hoặc cáp xoắn đôi
* Quy tắc xác định địa chỉ nguồn và đích để định vị thiết bị

1. Card Mạng (Ethernet Controller)?

* Là 1 bảng mạch được tích hợp sẵn trong bo mạch chủ của máy tính, nó nối trực tiếp với cổng Ethernet trên Case máy tính
* Máy tính muốn kết nối với Internet thì phải dùng 1 dây cáp Ethernet 1 đầu gắn vào cổng Ethernet trên Case rồi đầu kia gắn vào cổng Ethernet trên Modem hoặc Router, sau đó hệ điều hành sẽ tự động cài đặt Driver cho Card mạng, việc tiếp theo là truy cập Internet
* Card mạng trong Laptop hoặc điện thoại là Card mạng không dây, có 4 chế độ
* Ad Hoc, gửi truyền trực tiếp tín hiệu đến Card mạng khác không thông qua Access Point
* Monitor, không kết nối gì hết, nhưng lắng nghe tất cả sóng Wifi xung quanh
* Master, hoạt động như 1 Access Point
* Managed, chế độ mặc định, chỉ nhận và gửi dữ liệu thông qua Access Point, như bạn thấy là điện thoại của bạn chỉ kết nối với 1 Wifi hay chính là 1 Access Point
* Khi 1 Card mạng kết nối với 1 Access Point, thì khi này hiện tượng Handshake sẽ xảy ra, Card mạng gửi các gói tin mật khẩu tới Access Point để có thể truy cập nó

1. Modem?

* Giả sử nhà mạng cung cấp cho ta 1 cái ổ cắm, cắm vào ổ này là truy cập vào ổ này là truy cập được Internet, khi đó Modem sẽ là thiết bị đầu tiên cắm vào ổ này = cáp Ethernet, nó có tác dụng chuyển đổi dữ liệu Analog từ Internet sang Digital cho máy tính của bạn và ngược lại
* Trên Modem chỉ có 1 cổng Ethernet duy nhất để nối với 1 thiết bị khác giúp thiết bị này truy cập được Internet

1. Router?

* Vì nếu chỉ dùng Modem thì chỉ có duy nhất 1 thiết bị truy cập được Internet, nên phải dùng Router để giúp nhiều thiết bị truy cập Internet
* Nối Router với Modem = cáp Ethernet, sau đó nối các thiết bị có dây vào cổng trên Router = cáp Ethernet, các thiết bị không dây thì khỏi cần vì Router phát ra Wifi, như vậy tất cả thiết bị có thể truy cập Internet
* Bản chất khi dữ liệu từ Internet được gửi liên tục vào Modem, nhưng không phải dữ liệu nào cũng có đích đến là máy tính của bạn, Router có nhiệm vụ đọc địa chỉ đích đến của các gói tin, nếu địa chỉ là máy bạn thì nó nhận, không thì bỏ
* Ngoài ra, Router còn được dùng để định tuyến dữ liệu trên Internet, giống như trạm, để dữ liệu đi đúng tuyến đường cáp đến đúng máy đích
* Các thiết bị cùng kết nối với 1 Router sẽ giao tiếp được với nhau

1. Modem Wifi?

* Là Modem tích hợp cả Router, nhiều thiết bị có thể kết nối với Modem này thay vì 1 như trước kia

1. Switch?

* Nối nhiều thiết bị vào Switch, thì các thiết bị này giao tiếp được với nhau, nhưng Switch không có khả năng định tuyến và đọc địa chỉ để lọc gói tin giống Router, và không có chức năng phát Wifi
* Trong Router có Switch

1. Hub?

* Giống Switch, nhưng khi gói tin từ 1 máy gửi lên Hub, nó đéo quan tâm đích đến là máy nào mà gửi cho toàn bộ các máy kết nối với Hub

1. Access Point (AP)?

* Giống Hub, nhưng không cần nối dây
* Được coi là 1 điểm phát sóng Wifi

1. Server?

* Là 1 Host cực mạnh được cấu hình đặc biệt để lưu trữ tài nguyên như cơ sở dữ liệu, các tệp tin, ứng dụng, ...
* Có nhiệm vụ phân phát tài nguyên cho các Host con kết nối với nó khi có yêu cầu

Web:

1. Tên Miền Là Gì?

* Khi truy cập vào 1 trang Web, phần chữ trên thanh tìm kiếm, sau “https://” là tên miền

1. Cơ Chế Của Trình Duyện Web?

* Khi bạn nhập địa chỉ Web dưới dạng tên miền vào thanh tìm kiếm rồi nhấn Enter, đầu tiên trình duyệt Web sẽ lục soát trên Cache máy tính, nếu đã có 1 ánh xạ tên miền bạn nhập với địa chỉ IP tương ứng thì máy tính của bạn sẽ nhận được địa chỉ IP đó luôn, nếu không, máy tính của bạn sẽ gửi 1 yêu cầu thông qua Internet đến 1 DNS Resolver gần nhất, địa chỉ IP của DNS Resolver này được nhà mạng cấp cho
* Sau đó DNS Resolver lục soát Cache của nó, nếu đã có 1 ánh xạ tên miền bạn nhập với địa chỉ IP tương ứng thì nó trả về địa chỉ IP của trang Web cho máy tính của bạn luôn, nếu không, nó sẽ gửi yêu cầu lên Root Server gần nhất, có nhiệm vụ xác định phần đuôi của tên miền, ví dụ “.com”, và gửi địa chỉ IP của TLD Server ứng với phần đuôi “.com” lại cho DNS Resolver, sau đó DNS Resolver gửi yêu cầu đến TLD Server này, TLD Server này sẽ phân tích toàn bộ tên miền, ví dụ “foo.com”, rồi trả về địa chỉ IP của Authoritative Name Server tương ứng với địa chỉ IP này cho DNS Resolver và DNS Resolver lại tiếp tục gửi yêu cầu cho địa chỉ IP này, khi nhận được yêu cầu thì Authoritative Name Server sẽ lục soát trong đống ánh xạ của nó để tìm địa chỉ IP tương ứng với tên miền và trả về địa chỉ IP đó cho DNS Resolver
* Sau đó DNS Resolver lưu lại địa chỉ nhận được vào Cache của nó và đồng thời gửi cho máy tính của bạn, máy tính của bạn sau đó sẽ lưu lại địa chỉ IP này vào Cache và đồng thời gửi yêu cầu đến địa chỉ IP này
* Sau khi máy chủ có địa chỉ IP này nhận được yêu cầu nó sẽ trả về HTML, CSS, JS cho trình duyệt Web của bạn
* Có thể nhập trực tiếp địa chỉ IP lên trình duyệt Web để gửi yêu cầu nhưng đa số sẽ bị chặn

1. Cách thức hoạt động của Front End và Back End?

* Khi máy tính của bạn gửi yêu cầu lên Server, thì thực chất bạn đang gửi đến Port đang chạy Code Front End của Server, sau đó Front End sẽ gọi API tới 1 Port khác cũng trên Server đang chạy Back End, Port Back End trả về cơ sở dữ liệu cho Port Front End, sau đó Port Front End trả về HTML, CSS, … ứng với cơ sở dữ liệu nhận được từ Port Back End cho máy tính của bạn
* Khi Code Front End thì bạn không cần quan tâm Back End nó viết kiểu gì, chỉ cần quan tâm là thằng Back End sau khi làm phần Code của nó, nó sẽ đưa lên 1 Server tại 1 Port nào đó để chạy, và thằng Back End nó sẽ đưa cho bạn 1 cái API để bạn gọi tới Port này yêu cầu cơ sở dữ liệu, bạn cứ Code Front End như bình thường rồi đưa lên 1 Server nào đó với 1 Port nào đó khác với Back End để chạy, người dùng truy cập Web của bạn là đang gửi yêu cầu đến máy chủ Front End

1. TTL (Time To Live) Là Gì?

* Là thời gian để 1 ánh xạ tên miền vào địa chỉ IP tồn tại trong Cache của DNS Resolver trước khi bị xóa, được đặt giá trị bởi quản trị viên

1. Cách DNS Resolver Lưu Địa Chỉ IP Động?

* Nó sẽ tự động cập nhật ánh xạ tên miền với địa chỉ IP khi có sự thay đổi địa chỉ IP, DNS Resolver dạng này gọi là DDNS Resolver

1. Cách Hoạt Động Của Các Phương Thức Get, Post, …?

* Khi 1 máy khách gửi yêu cầu lên máy chủ, nó có thể là yêu cầu trả về giao diện trang Web, hay thêm 1 bản ghi vào cơ sở dữ liệu, hay chỉnh sửa bản ghi, …, mỗi kiểu yêu cầu sẽ tương ứng với 1 phương thức khác nhau
* Khi máy khách gửi yêu với phương thức Get, máy chủ sẽ nhận yêu cầu, và trả về HTML, CSS, ... cho máy khách, cách trả về như nào thì do lập trình viên Back End quy định, khi vừa vào 1 tuyến đường là mách khách đang thực hiện phương thức Get
* Khi máy khách gửi yêu cầu với phương thức Post, máy chủ sẽ nhận yêu cầu và thêm 1 bản ghi do người dùng nhập vào, thêm bản ghi như nào thì do lập trình viên Back End quy định

Model:

1. Mô Hình OSI (Open Systems Interconnection)?

* Gồm 7 tầng, dữ liệu sẽ đi qua từng tầng một
* Application (ứng dụng)
* Presentation (trình bày)
* Session (phiên)
* Transport (truyền tải), sửa lỗi tin, chia nhỏ tin để truyền, hợp tin, mỗi gói tin nhỏ sẽ được bọc thêm Transport Header tạo thành Segment
* Network (mạng), phân giải IP, tìm đường gửi nhận tin, gồm Router, mỗi Segment được thêm Network Header tạo thành Packet
* Data Link (Network Access, MAC, liên kết dữ liệu), kết nối các thiết bị trong cùng mạng, gồm Switch, mỗi Packet được thêm Frame Header và Frame Trailer tạo thành Frame
* Physical (vật lý), gồm các thiết bị như máy tính, …
* Sau khi dữ liệu đi qua hết tầng để đến máy thứ 2, nó sẽ đi ngược lại 7 tầng

1. Mô Hình TCP/IP (Transmission Control Protocol / Internet Protocol)?

* Giống OSI, nhưng 3 tầng đầu gộp chung lại thành Application
* 2 tầng đặc trưng là Transport = TCP và Network = IP

1. Điện Toán Biên (Edge Computing)?

* Là đặt siêu máy tính ngay cạnh cảm biến để tính toán, giảm độ trễ khi truyền dữ liệu

1. Mô hình IOT?

* Gồm 5 tầng
* Do (làm), gồm các xe, Robot tự hành
* Learn (học), học sâu
* Collect (thu thập), gồm Server, dữ liệu được đẩy lên Server để xử lí
* Connect (kết nối), gồm các tiêu chuẩn kết nối như Bluetooth, …, các giao thức giao tiếp phải đảm bảo 1 đứa truyền thì mấy đứa khác phải im, sử dụng phần mềm OMNeT để mô phỏng mạng
* Things (vật), gồm các cảm biến, … giá thành thấp, sống lâu, dễ sử dụng, giao tiếp với nhau bằng giao thức MQTT

Anti Virus:

1. Tường Lửa (Firewall)?

* Bản chất là 1 tấm lá chắn đặt trước máy tính của bạn
* Khi có dữ liệu truyền tới máy tính của bạn, có thể là từ Internet, nó phải qua tường lửa trước, khi này, tường lửa sẽ lọc dữ liệu nào được gửi đến máy của bạn, dữ liệu nào không

1. Các Loại Phần Mềm?

* Software = phần mềm cấp cao mức độ giao diện
* Firmware = phần mềm cấp thấp dùng để điều khiển các phần cứng trong máy như bảng mạch thu phát Wifi
* Malware = phần mềm độc hại
* Freeware = phần mềm miễn phí (phải đáp ứng 1 số điều kiện)
* Shareware = phần mềm độc quyền (ban đầu cho dùng thử sau tính phí)
* Ransomware = phần mềm tống tiền (chặn truy cập cho tới khi trả tiền)

Kali Linux:

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
* Ngoài tài khoản người dùng bạn mới tạo, còn có tài khoản mặc định là Root, là tài khoản có quyền tối cao làm bất cứ thứ mình muốn với hệ thống
* Sẽ có 2 giao diện lệnh chính là Terminal và Power Shell
* Trong Terminal, để chạy lệnh với tư cách Root thì thêm sudo ở đầu, hoặc mở Root Terminal
* Để mở nhanh Terminal, nhấn “Ctrl” + “Alt” + “T”

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 Terminal gõ lệnh

sudo update-grub

sudo 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

* 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, nên nhấn “Ctrl” + “H” để hiện
* Mặc định khi mở Terminal thì nó ở thư mục kí hiệu Root, kí hiệu “~”, từ Root, để vào thư mục con cháu của nó thì trước tiên nhập lệnh sau

cd /

* Ở trạng thái này, lệnh cd giống trong Batch
* Để trở lại “~”

cd ~

* Hoặc

cd root

* 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 khi không có phần mở rộng
* Thuần văn bản, “Plain text document”, biểu tượng tờ giấy có văn bản
* File thực thi, “Executable”, biểu tượng bánh răng

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 đầu hiển thị thông tin về 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 bắt đầu lắng nghe các gói tin của 1 Wifi nào đó

airodump-ng -c 5 -w wifi –bssid <BSSID Của Wifi> <Tên Card Mạng Monitor>

* Ví dụ

airodump-ng -c 5 -w wifi –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

“wifi-<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 “wifi-01” và “wifi-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

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

* Vào Terminal, nhập

fdisk -l

1. Hiện Thông Tin Người Dùng Hiện Tại?

* Vào Terminal, nhập

who

1. Hiện Nội Dung Trong 1 File Vào Terminal?

* Vào Terminal, nhập

cat <Đường Dẫn Tới File Không Cần Phần Mở Rộng>

* Ví dụ

cat /home/foo

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>

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>

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

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. Desktop?

* Gồm nhiều trang, đánh số thứ tự là 1, 2, 3, 4, … ở thanh trên cùng tay trái
* 1 trang sẽ mở các chương trình khác nhau
* Có thể chuyển qua lại giữa các trang

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>

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

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