Lê Cảnh Giang Thi

TRAINING WEB

1. Ngày 3/6: Internet
2. Internet là gì?

Inter: among, between

Net: network

* Hệ thống các mạng kết nối với nhau trên toàn cầu

A diagram of a network

Description automatically generated

Hình minh họa Internet (hình thành từ nhiều mạng, mỗi cục là 1 mạng)

ISP: giống như 1 nhà mạng. Regional ISP: VNPT, Viettel…

Switch: cái cục để nối các máy vào 1 mạng

Mạng nhà có Wi-fi vì cho điện thoại xài, điện thoại ko cắm LAN được

***Mô hình OSI (Open System Interconnection)***

Appilication: Cung cấp giao diện để user tương tác với mạng

Presentation: Lớp xử lý data khi gửi lên mạng, mã hóa dữ liệu nhập vào (encrypt), chuyển xuống các lớp dưới.

Session: Quản lý kết nối giữa các app với nhau (phiên bản, cookie nằm trong session)

Transport: protocol nằm ở dưới cùn, hỗ trợ vận chuyển các gói data để thiết lập các protocol cao hơn

Network: IP, routers của mình

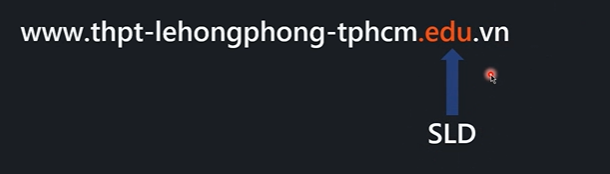
Data link: Điều hướng IP cho nó đi (vd: switches, Ethernet); là địa chỉ của mình ở trên mạng; tương tự MAC address. Provides node-to-node data transfer , error detection and correction.

Physical: dây cáp

A screenshot of a computer

Description automatically generated

Mô hình OSI và chức năng



A screen shot of a computer

Description automatically generated

Mô hình hiển thị 1 tin nhắn (vd) từ PC1 sang PC2

1. Protocol (DNS, HTTP,…)
2. DNS – Domain Name System

A black and white screen with white text

Description automatically generated

Domain: tên miền, địa chỉ để truy cập vào trang web

A black background with white text

Description automatically generated

Top Level Domain (.com, .vn, .usuk…)

.edu: SLD (Second Level domain)

www: Sub Domain (ko có quy ước)

thpt-lehongphong-tphcm: Third Level Domain

Dấu (.) cuối cùng : Root, ko hiện ra

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Khi nhập tên 1 domain vào search, browser sẽ kiểm tra trên cache (bộ nhớ tạm) rồi hỏi hệ điều hành (operating system - OS), nếu OS biết thì trả lại, còn nếu OS ko biết thì hỏi DNS Resolver, DNS Resolver kiểm tra cache của nó, cache cũng ko thấy thì Resolver đi hỏi Internet Service Provider (ISP, nhà mạng), rồi ISP kiểm tra cache của nó mà ko thấy nữa thì ISP đi hỏi Top Level Domain (.vn) bằng cách ISP đi tới Root name server (vì biết .vn chứ 0 biết .vn ở đâu), kiếm đc địa chỉ IP của TLD thì Root name server trả địa chỉ IP của TLD về ISP. TLD sẽ trả về cho ISP 1 ANS (authoritative name server – quản lý domain) rồi trả về ISP cái IP; rồi trả về theo từng thứ tự còn lại (ISP, DNS, OS, Browser).

Nếu nhập thẳng IP (ko phải domain) thì đi thẳng tới trang web đó luôn, ko phải qua DNS nữa.

Phải theo quy trình phức tạp như vậy vì domain mới phải cập nhật. Mấy trăm cái máy tính lưu domain.

Làm sao TLD biết đc server nào giữ domain của mình trong khi nó ko biết domain của mình tương ứng với IP nào?

* Khi đăng ký domain thì có 1 list authoritative name server được gửi tới TLD để quản lý. TLD ko cần biết domain của mình là gì, nó chỉ cần biết do thằng nào giữ thôi. (Glue Record)

1. HTTP (HypetText Transfer Protocol)

* Protocol là những bước bắt đầu cuộc trò chuyện – thủ tục.

A diagram of a text transfer protocol

Description automatically generated

A screen shot of a computer

Description automatically generated

TCP: Kết nối máy tính với server (2 chiều).

A black background with white arrows

Description automatically generated

2 cái cuối: 1 là request của mình, 2 là respond của server.

A screenshot of a computer

Description automatically generated

Ở trên: request, ở dưới: respond

Kiểu dữ liệu của HTTP là văn bản.

A screenshot of a computer

Description automatically generated

HTTP là chuỗi ký tự qua TCP, HTTP ở application còn TCP ở transport. Kiểu dữ liệu: plaintext

HTTPS: HYPERTEXT TRANSFER PROTOCOL SECURE

A screenshot of a computer screen

Description automatically generated

Cài đặt TLS (Transport Layer Security) thì mã hóa request ban đầu và respond nên ko thể đọc được.

Sơ đồ mã hóa respond – request trên private key và public key

A screen shot of a computer

Description automatically generated

Nếu có máy thứ 3 thì đột nhập thì sẽ lấy được public key nhưng ko có private key; trong khi phải kết hợp cả 2 key thì mới mã hóa được.

Mình có public key, mình mã hóa -> gửi public key cho server. Server đã có private key -> giải mã request và gửi ngược lại public key của server cho mình. Mình dùng private key của mình để giải mã respond. Để mã hóa thì chỉ cần public key nhưng để giải mã thì cần cả 2.