**Domain Name System Security – Bảo mật DNS**

Máy chủ thường là mục tiêu tấn công đầu tiên của các hacker nhằm đánh cắp thông tin và gây hại cho hệ thống an ninh của doanh nghiệp. **Domain Name System Security** chính là giải pháp giúp xác định các địa chỉ IP độc hại trên internet mà máy chủ truy cập.

## **Domain Name System là gì?**

**Domain Name System** được viết tắt là DNS, là hệ thống phân giải tên miền được phát minh vào năm 1984 cho Internet, là hệ thống giúp chuyển đổi tên miền sang các địa chỉ IP tương ứng. DNS cho phép thiết lập, liên kết với các trang thiết bị mạng với mục đích định vị và địa chỉ hóa các thiết bị trên nền tảng internet.

Các tên miền trên internet được mã hóa dưới hình thức là địa chỉ IP (123.4.56.567), vì vậy nếu không có DNS thì người dùng phải truy vấn dãy số IP trên công cụ tìm kiếm. Hệ thống DNS ra đời giúp chuyển đổi tên miền dễ nhớ (vietnetco.vn) thành địa chỉ IP và ngược lại trong quá trình truy xuất dữ liệu tìm kiếm trên internet. Nhờ vậy mà người dùng chỉ cần nhớ các tên miền để tìm kiếm dữ liệu chứ không cần phải ghi nhớ các địa chỉ IP của tên miền.

Hệ thống tên miền bao gồm một loạt các cơ sở dữ liệu (CSDL) chứa địa chỉ IP và các tên miền của nó. Hệ thống tên miền phát triển dưới dạng các CSDL phân tán. Mỗi CSDL này sẽ quản lý một phần trong hệ thống tên miền..

### **Cấu trúc của Domain Name System**

* Domain Name Space: là không gian tên miền có cấu trúc dạng cây chứa nhiều node có gắn nhãn. Chúng lưu trữ thông tin liên quan đến Domain Name
* Domain Name: Tên miền bao gồm các nhãn và phân cách bằng dấu “.”. Ví dụ: vietnetco.vn. Ngoài ra Domain Name cũng chia ra nhiều cấp độ khác nhau gọi là Top level, tên miển cấp 2, 3, …
* Domain Name Syntax: Gọi là cú pháp của tên miền. Hệ thống DNS sẽ phân giải tên miền từ trái sang phải theo cấu trúc cú pháp của tên miền. Ví dụ cú pháp tên miền: www.vietnetco.vn
* Name Server: Đây là máy chủ của tên miền sẽ chứa thông tin không gian tên miền. Mỗi tên miền sẽ có ít nhất 1 Name Server chứa thông tin của tên miền đó
* Internationalized domain names: tên miền Quốc tế hóa được hình thành do sự giới hạn của bộ kí tự ASCII trong diễn tả các ngôn ngữ khác nhau.
* Authoritative name server: Với máy chủ tên miền thẩm quyền, có thể trả lời các truy vấn DNS từ dữ liệu gốc

### **Nguyên tắc hoạt động của Domain Name System**

Mỗi Doanh nghiệp sẽ thiết lập và duy trì một DNS server riêng. Khi trình duyệt thực hiện truy vấn đia chỉ tên miền của 1 website thì DNS server của chính doanh nghiệp sẽ tiến hành phân giải. DNS server của các tổ chức khác sẽ không thực hiện được.

**Domain Name System** có thể truy vấn được các DNS Server khác để có được tên phân giải. Mỗi DNS Server sẽ thực hiện 2 nhiệm vụ là phân giải tên miền trong dữ liệu của chúng về các địa chỉ IP và cung cấp thông tin cho các DNS Server khác trong quá trình phân giải của các DNS Server này.

Quá trình phân giải tên miền DNS sẽ trải qua 8 bước:

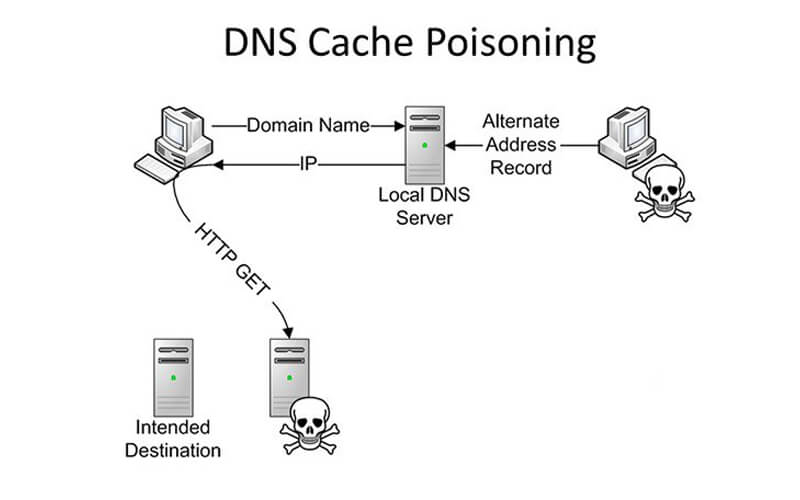
* 1. Người dùng nhập ‘vietnetco.vn’ vào trình duyệt web và truy vấn sẽ truyền vào Internet và được nhận bởi trình phân giải đệ quy DNS.
  2. Trình phân giải sẽ truy vấn một máy chủ định danh gốc DNS (.).
  3. Máy chủ gốc sẽ phản hồi với trình phân giải bằng địa chỉ của máy chủ DNS của Miền cấp cao nhất (TLD) (chẳng hạn như .com hoặc .net), nơi lưu trữ thông tin cho các miền của nó. Khi tìm kiếm vietnetco.vn, yêu cầu của chúng tôi được hướng tới TLD .vn.
  4. Trình phân giải đưa ra yêu cầu tới .com TLD.
  5. Máy chủ TLD sẽ phản hồi bằng địa chỉ IP của máy chủ định danh của miền, example.com.
  6. Cuối cùng, trình phân giải đệ quy gửi một truy vấn đến máy chủ định danh của miền.
  7. Địa chỉ IP cho example.com sau đó được trả về trình phân giải từ máy chủ định danh.
  8. Sau đó, trình phân giải DNS sẽ phản hồi lại trình duyệt web bằng địa chỉ IP của miền được yêu cầu ban đầu.

Sau khi 8 bước tra cứu DNS đã trả lại địa chỉ IP cho vietnetco.vn, trình duyệt có thể thực hiện yêu cầu cho trang web:

1. Trình duyệt thực hiện một yêu cầu HTTP đến địa chỉ IP.
2. Máy chủ tại IP đó trả về trang web sẽ được hiển thị trong trình duyệt (bước 10).

## **Ảnh hưởng của Domain Name System Security đến hệ thống mạng?**

Với bản chất là dịch vụ truy vấn có cấu trúc phân tán, có khả năng mở rộng gần như không giới hạn, hệ thống **Domain Name System Security** được ra đời với mục đích chính là để truy vấn địa chỉ IP từ một tên miền. Mỗi Website có một tên và một địa chỉ IP. Địa chỉ IP gồm 4 nhóm số cách nhau bằng dấu chấm (IPv4). Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập địa chỉ IP của trang web.



Quá trình “dịch” tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một DNS server. Các DNS trợ giúp qua lại với nhau để dịch địa chỉ “IP” thành “tên” và ngược lại. Người sử dụng chỉ cần nhớ “tên”, không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ).

Do tầm ảnh hưởng của Domain Name System Security cực kỳ quan trọng với hệ thống mạng nên có rất nhiều tấn công nhằm vào hệ thống này. Một trong những dạng tấn công phổ biến

* Giả mạo master trong việc đồng bộ dữ liệu giữa các máy chủ DNS.
* Spoofing master, spoofing update, …
* Chuyển hướng phân giải DNS người dùng sang DNS giả mạo: Man in middle attack.
* Đầu độc bộ nhớ Cache DNS: DNS Cache Poisoning hay DNS Pharming
* Giả mạo hoặc thay đổi các bản ghi trong DNS.

## **Chức năng của giải pháp Domain Name System Security**

Giải pháp bảo mật **Domain Name System Security** giúp đảm bảo và bảo vệ cho việc truy cập các ứng dụng trên Cloud hoặc trong mạng nội bộ của người dùng. Giải pháp cung cấp những tính năng chính sau:

* Quản trị tập trung trên nền tảng duy nhất: Cung cấp công cụ giám sát IP của các thiết bị, máy ảo và hệ thống máy chủ DNS – DHCP xuyên suốt cho hệ thống mạng nội bộ hoặc các ứng dụng cloud.
* Bảo vệ DNS toàn diện: Nhận diện tấn công mạo danh dữ liệu DNS thông qua bộ lọc nội dung dữ liệu.
* Thiết kế, triển khai và quản lý đơn giản cho hệ thống máy chủ DNS và DHCP đa nền tảng trên kiến trức hợp nhất
* Hỗ trợ tích hợp với các bên thứ 3 thông qua API để tăng cường bảo mật cho hệ thống.