BỘ GIÁO BỘ GIÁO DỤC VÀ ĐÀO TẠO

ĐẠI HỌC ĐÀ NẴNG

-----□ -----

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGÀNH KHOA HỌC MÁY TÍNH

(Theo định hướng ứng dụng)

Mã số: 60.48.01

TÊN ĐỀ TÀI

XÂY DỰNG GIẢI PHÁP

PHÒNG CHỐNG TẤN CÔNG DỊCH VỤ

TRONG MẠNG VNPT QUẢNG BÌNH

Tên HV:

CBHD: TS. Lê Thị Mỹ Hạnh

Lớp: KHMT – K34

Đồng Hới, 04/2018

LỜI CẢM ƠN

Trước tiên tôi xin bày tỏ lòng biết ơn sâu sắc tới cô giáo TS. Lê Thị Mỹ Hạnh đã tận tình hướng dẫn trong suốt thời gian nghiên cứu và hoàn thành luận văn này.

Tôi cũng xin cảm ơn Ban lãnh đạo Đại học Đà Nẵng, Khoa Công nghệ Thông tin, cũng như các đồng nghiệp đã tạo điều kiện và giúp đỡ tôi hoàn thành được đề tài nghiên cứu của mình.

Cuối cùng là sự biết ơn tới gia đình, đồng nghiệp, bạn bè lớp cao học K34_KHMT_QB đã thông cảm, động viên giúp đỡ cho tôi trong quá trình học tập và thực hiện luận văn.

Đồng Hới, ngày tháng năm 2018

NGUYỄN THA

LỜI CAM ĐOAN

Tôi xin cam đoan nội dung luận văn của tôi là do sự tìm hiểu và nghiên cứu của bản thân. Các kết quả nghiên cứu cũng như ý tưởng của các tác giả khác đều được trích dẫn cụ thể. Đề tài luận văn của tôi chưa được bảo vệ tại bất kỳ một hội đồng bảo vệ luận văn thạc sĩ nào trong nước và nước ngoài.

Tác giả

NGUYỄN THA

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Thuật ngữ	Tiếng Anh	Tiếng Việt
ccTLD	Country code top – level domain	Tên miền quốc gia cấp cao nhất
CNAME	Canonical Name	Tên chuẩn
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ
DNS	Domain Name System	Hệ thống tên miền
DNSSEC	The Domain Name System Security Extensions	Hệ thống tên miền bảo mật mở rộng
Dos	Denial of Service	Tấn công từ chối dịch vụ
ICANN	The Internet Corporation for Assigned Names anh Number	Tổ chức quản lý hệ thống tên miền trên thế gới
INTERNIC	Internet Network Information Center	Trung tâm thông tin mạng Quốc tế
IPV4	Internet Protocol Version 4	Giao thức liên mạng thế hệ 4
IPV6	Internet Protocol Version 6	Giao thức liên mạng thế hệ 6
LIFO	Last in first out	Vào sau ra trước
NSF	National Science Foundation	Quỹ khoa học quốc gia
URL	Uniform Resource Locator	Định vị tài nguyên thống nhất
TLD	Top – Level Domain	Tên miền cấp cao nhất
TTL	Time To Live	Thời gian cập nhật
VPN	Virtual Private Network	Mạng riêng ảo

DANH MỤC HÌNH VẼ

LỜI MỞ ĐẦU

Tính cấp thiết của đề tài:

Trong những thập kỷ gần đây, thế giới và Việt Nam đã và đang chứng kiến sự phát triển bùng nổ của công nghệ thông tin, truyền thông. Đặc biệt sự phát triển của các trang mạng (websites) và các ứng dụng trên các trang mạng đã cung cấp nhiều tiện ích cho người sử dụng từ tìm kiếm, tra cứu thông tin đến thực hiện các giao dịch cá nhân, trao đổi kinh doanh, mua bán, thanh toán hàng hoá, dịch vụ, thực hiện các dịch vụ công... Tuy nhiên, trong sự phát triển mạnh mẽ của các trang mạng nói riêng và công nghệ thông tin nói chung, vấn đề đảm bảo an toàn, an ninh thông tin cũng trở thành một trong những thách thức lớn. Một trong những nguy cơ tác động đến việc đảm bảo an toàn thông tin trong nhiều năm qua chưa được giải quyết đó chính là các hoạt động tấn công thiết bị IoT, một thủ đoạn phổ biến của tội phạm nhằm cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số.

Với sự phát triển internet bùng nổ như hiện nay, đặc biệt tại Quảng Bình, VNPT hiện là nhà cung cấp dịch vụ có thị phần lớn nhất, với hơn 60.000 khách hàng đang sử dụng dịch vụ băng rộng hữu tuyến internet của VNPT Quảng Bình. Bên cạnh việc không ngừng nâng cao chất lượng dịch vụ, chính sách giá cước,

VNPT Quảng Bình còn xây dựng nhiều phương án để tăng cường bảo mật thông tin cho khách hàng.

Trong bối cảnh các hệ thống thông tin phục vụ cho xây dựng Chính phủ điện tử, thành phố thông minh sẽ sử dụng ngày càng nhiều các hệ thống, thiết bị nối thiết bị IoT để phục vụ cho những nhu cầu thiết yếu của người dân, rõ ràng kèm theo đó các nguy cơ mất an toàn thông tin mạng sẽ lớn hơn nhiều và mức độ thiệt hại do các cuộc tấn công mang cũng sẽ gia tăng theo cấp số nhân.

Để nâng cao chất lượng dịch vụ cho khách hàng, đặc biệt đảm bảo mật thông tin cho khách hàng hiện tại và tương lai của VNPT, tôi đã lựa chọn đề tài :

"Xây dựng giải pháp phòng chống tấn công dịch vụ trong mạng VNPT Quảng Bình", với mục đích xây dựng, kiểm thử một số giải pháp sử dụng thực tế, phần mềm mã nguồn mở để các công ty vừa và nhỏ có thể triển khai dễ dàng.

Tổng quan về vấn đề nghiên cứu:

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên được phát minh vào năm 1984 cho Internet. Hệ thống tên miền (DNS) về căn bản là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ (dạng ký tự, ví dụ www.example.com) sang địa chỉ IP vật lý (dạng số, ví dụ 123.11.5.19) tương ứng của tên miền đó. DNS giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

Phép so sánh thường được sử dụng để giải thích cho DNS là, nó phục vụ như một "Danh bạ điện thoại", có khả năng tìm kiếm và dịch tên miền thành địa chỉ IP. Ví dụ, www.example.com dịch thành 208.77.188.166. Tên miền Internet dễ nhớ hơn các địa chỉ IP, là 208.77.188.166 (IPv4) hoặc 2001: db8: 1f70:: 999: de8: 7648:6 e8 (IPv6).

Hệ thống tên miền phân phối trách nhiệm gán tên miền và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền. Những máy chủ có tên thẩm quyền được phân công chịu trách nhiệm đối với tên miền riêng của họ, và lần lượt có thể chỉ định tên máy chủ khác độc quyền của họ cho các tên miền phụ. Kỹ thuật này đã thực hiện các cơ chế phân phối DNS, chịu

đựng lỗi, và giúp tránh sự cần thiết cho một trung tâm đơn lẻ để đăng ký được tư vấn và liên tục cập nhật.

DNS là chìa khóa chủ chốt của nhiều dịch vụ mạng như duyệt internet, mail server, web server…Nếu không có DNS, internet sẽ mau chóng lụi tàn, từ đó có thể hình dung được mức độ quan trọng của DNS. Và việc tấn công dịch vụ DNS ngày càng được nhiều hacker sử dụng với mục đích kinh tế, chính trị với nhiều hình thức mới và tinh vi.

Mục đích nghiên cứu:

Nghiên cứu tìm hiểu về DNS, phân loại DNS, giới thiệu một số công cụ tấn công DNS và các giải pháp phòng chống DNS mà về mặt chủ quan học viên nhận thấy được tính khả thi. Dựa trên các giải pháp đã trình bày xây dựng một số kịch bản kiểm thử việc ngăn chặn tấn công DNS với mục tiêu là các thiết bị truy nhập của khách hàng.

Đối tượng và phạm vi nghiên cứu:

Nghiên cứu về các loại hình tấn công từ chối dịch vụ phân tán và một số giải pháp dựa trên các công cụ hiện có. Từ đó học viên cài đặt và kiểm thử giải pháp có giá thành rẻ, dễ triển khai với cá nhân và các doanh nghiệp vừa và nhỏ.

Phương pháp nghiên cứu:

+ *Nghiên cứu lý thuyết, phân tích tài liệu*: Học viên thu thập tài liệu, bài báo và các báo cáo tổng quan về DNS, nghiên cứu các phương pháp bất thường khi tấn công dịch vụ DNS.

+ *Nghiên cứu thực nghiệm:* Cài đặt mô phỏng một cuộc tấn công trong hệ thống mạng. Thực hiện đánh giá, phân tích kết quả và cuối cùng là đề xuất các biện pháp phòng chống, chống tấn công DNS.

Luận văn bao gồm 3 chương :

- ***Chương I.* Tổng quan về hệ thống tên miền DNS:** Trình bày một cách tổng quan về hệ thống tên miền DNS, chức năng của DNS và cơ chế phân giải tên miền và địa chỉ IP.

- ***Chương II*. Phân tích các cách thức tấn công DNS:** Trình bày các lỗ hổng, các điểm yếu bảo mật trong DNS và các cách thức tấn công vào hệ thống DNS mà các hacker thường sử dụng hiện nay.

- ***Chương III*. Cài đặt và thử nghiệm một số kiểu tấn công và giải pháp phòng chống tấn công:** Trình bày mô hình thực tế, giải pháp, mô hình thực nghiệm trong mạng VNPT Quảng Bình và quá trình kiểm tra đánh giá, nhận xét hệ thống phòng chống xâm nhập.

CHƯƠNG 1. TỔNG QUAN VỀ HỆ THỐNG TÊN MIỀN DNS

1.1. GIỚI THIỆU HỆ THỐNG TÊN MIỀN DNS

1.1.1. Giới thiệu chung về DNS:

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống tên miền được phát minh vào năm 1984 cho Internet, định nghĩa trong các RFC 1034 và 1035, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống tên miền (DNS) là một hệ thống đặt tên theo thứ tự cho máy vi tính, dịch vụ, hoặc bất kì nguồn lực tham gia vào Internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho những người tham gia. Quan trọng nhất là nó chuyển tên miền có ý nghĩa cho con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới [1].

Hệ thống tên miền (DNS) là nền tảng của Internet giúp người dùng dễ dàng đặt tên dựa trên tài nguyên Records (RR) vào các địa chỉ IP tương ứng và ngược lại. Nhưng ngày nay DNS không chỉ là địa chỉ dịch mà nó còn cung cấp xác thực và cải thiện an ninh dịch vụ của nhiều ứng dụng internet. Bây giờ DNS trở thành thành phần quan trọng nhất của Internet. Nếu DNS không hoạt động bình thường thì toàn bộ truyền thông trong internet sẽ sụp đổ. Vì vậy an ninh của cơ sở hạ tầng DNS là một trong những yêu cầu cốt lõi đối với bất kỳ tổ chức nào.[1]

DNS là nơi yêu thích của kẻ tấn công do sự mất mát lớn khi DNS bị tấn công Kết quả, DNS sẽ sụp đổ dẫn đến tất cả các máy chủ và internet cũng sụp đổ theo. Các ứng dụng được xuất bản qua internet từ đó cũng ngưng hoạt động. Do đó các vi phạm trong an ninh DNS sẽ dẫn đến ảnh hưởng sự tin cậy của internet. Vì vậy, bảo mật của DNS là tối quan trọng, trong trường hợp cơ sở hạ tầng DNS là tổ chức bị tổn hại sẽ dẫn đến mất doanh thu, làm giảm độ tin cậy của họ do thời gian chết, sự không hài lòng của khách hàng, mất mát riêng tư, đối đầu với những thách thức pháp lý. DNS (Tên miền Name System) là lập bản đồ phân cấp cơ sở dữ liệu động nằm rải rác trên toàn cầu cung cấp nhiều dịch vụ liên quan đến internet [1].

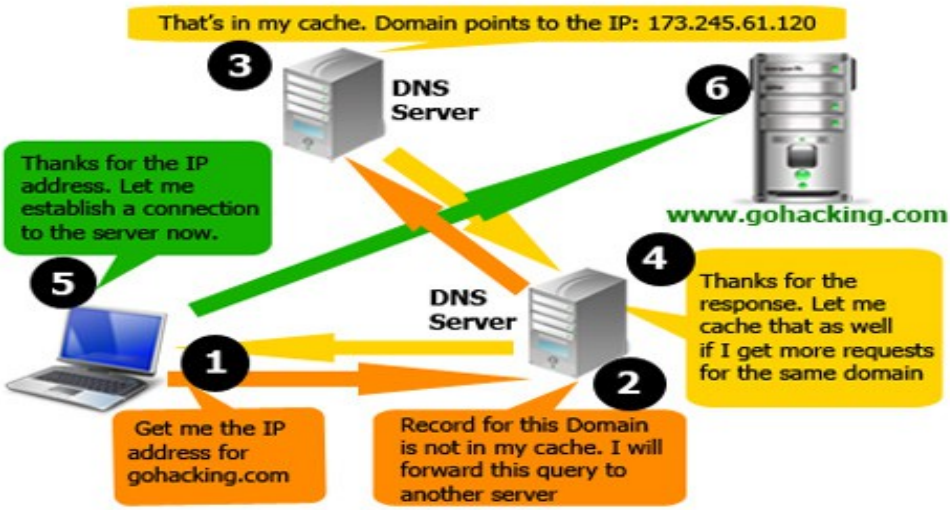
*1.1.2. **Nguyên tắc làm việc của DNS***

Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server riêng của mình, gồm các máy bên trong phần riêng của mỗi nhà cung cấp dịch vụ đó trong Internet. Tức là, nếu một trình duyệt tìm kiếm địa chỉ của một website thì DNS server phân giải tên website này phải là DNS server của chính tổ chức quản lý website đó chứ không phải là của một tổ chức (nhà cung cấp dịch vụ) nào khác.

INTERNIC (Internet Network Information Center) chịu trách nhiệm theo dõi các tên miền và các DNS server tương ứng. INTERNIC là một tổ chức được thành lập bởi NSF (National Science Foundation), AT&T và Network Solution, chịu trách nhiệm đăng ký các tên miền của Internet. INTERNIC chỉ có nhiệm vụ quản lý tất cả các DNS server trên Internet chứ không có nhiệm vụ phân giải tên cho từng địa chỉ.

DNS có khả năng truy vấn các DNS server khác để có được 1 cái tên đã được phân giải. DNS server của mỗi tên miền thường có hai việc khác biệt. Thứ nhất, chịu trách nhiệm phân giải tên từ các máy bên trong miền về các địa chỉ Internet, cả bên trong lẫn bên ngoài miền nó quản lý. Thứ hai, chúng trả lời các DNS server bên ngoài đang cố gắng phân giải những cái tên bên trong miền nó quản lý.

DNS server có khả năng ghi nhớ lại những tên vừa phân giải. Để dùng cho những yêu cầu phân giải lần sau. Số lượng những tên phân giải được lưu lại tùy thuộc vào quy mô của từng DNS [3].

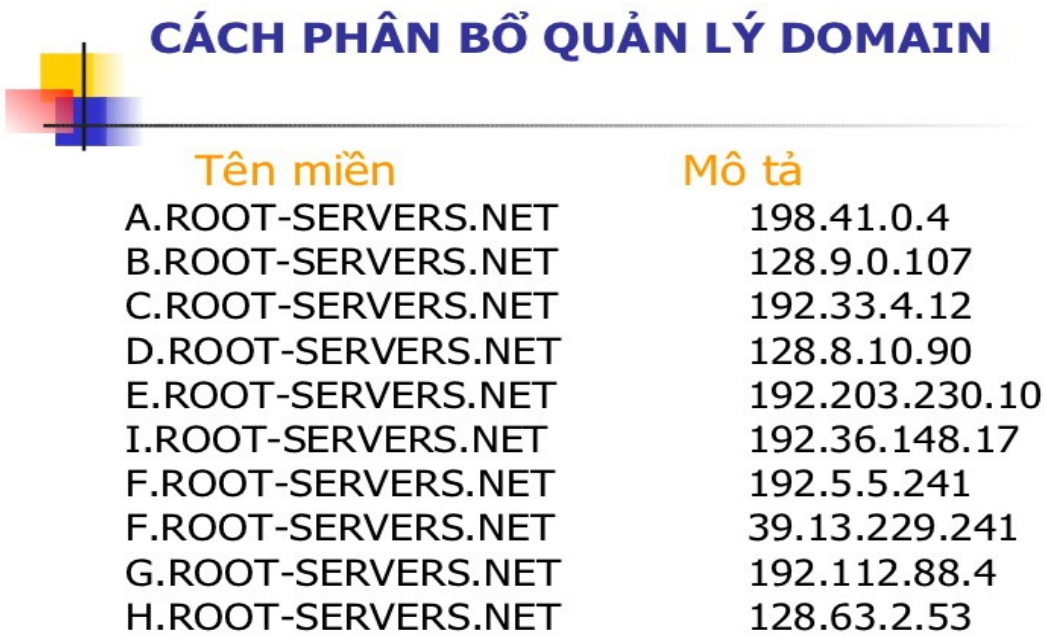


Hình 1-1: Nguyên tắc làm việc của DNS

Do các DNS có tốc độ biên dịch khác nhau, có thể nhanh hoặc có thể chậm, do đó người sử dụng có thể chọn DNS server để sử dụng cho riêng mình. Có các cách chọn lựa cho người sử dụng. Sử dụng DNS mặc định của nhà cung cấp dịch vụ (Internet), trường hợp này người sử dụng không cần điền địa chỉ DNS vào network connections trong máy của mình. Sử dụng DNS server khác (miễn phí hoặc trả phí) thì phải điền địa chỉ DNS server vào network connections. Địa chỉ DNS server cũng là 4 nhóm số cách nhau bởi các dấu chấm.

1.2. CÁCH PHÂN BỐ DỮ LIỆU, CẤU TRÚC GÓI TIN DNS

Những root name server (.) quản lý những top-level domain trên Internet. Tên máy và địa chỉ IP của những name server này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những name server này cũng có thể đặt khắp nơi trên thế giới [ ].



Hình 1-2: Cách phân bố quản lý domain

Thông thường, một tổ chức được đăng ký một hay nhiều domain name. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều name server và duy trì cơ sở dữ liệu cho tất cả những máy tính trong domain. Những name server của tổ chức được đăng ký trên Internet. Một trong những name server này được biết như là Primary Name Server. Nhiều Secondary Name Server được dùng để làm backup cho Primary Name Server. Trong trường hợp Primary bị lỗi, Secondary được sử dụng để phân giải tên.

Primary Name Server có thể tạo ra những subdomain vf ủy quyền những subdomain này cho những Name Server khách. Subdomain rất hữi ích cho các tổ chức và namespace lớn.

DNS có cấu trúc phân cấp. Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây. Với .Root server là đỉnh của cây và sau đó các miền (domain) được phân nhánh dần xuống phía dưới và phân quyền quản lý. Khi một máy khách (client) truy vấn một tên miền nó sẽ đi lần lượt từ root phân cấp xuống dưới để đến DNS quản lý domain cần truy vấn. Tổ chức quản lý hệ thống tên miền trên thế giới là The Internet Corporations for Assigned Names and Numbers

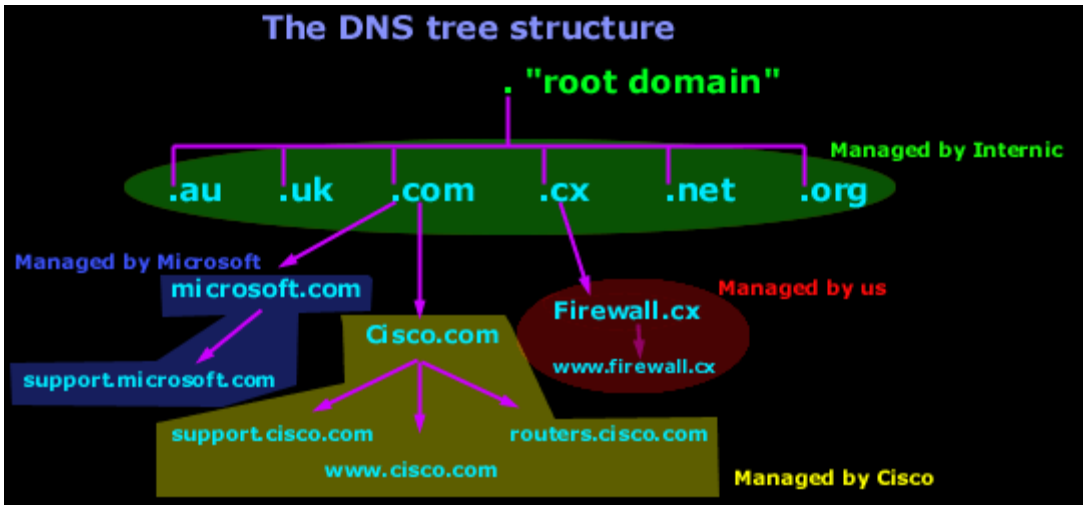
(ICANN). Tổ chức này quản lý mức cao nhất của hệ thống tên miền (mức root) do đó nó có quyền cấp phát các tên miền ở mức cao nhất gọi là Top-Level-Domain.

Cấu trúc của dữ liệu được phân cấp hình cây root quản lý toàn bộ sơ đồ và phân quyền quản lý xuống dưới và tiếp đó các tên miền lại được chuyển xuống cấp thấp hơn.

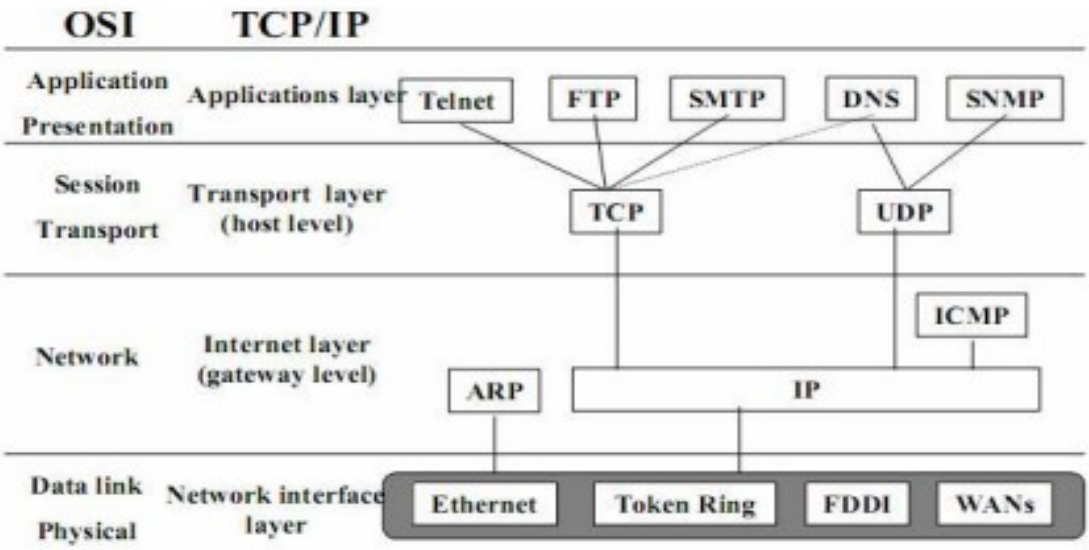
Hệ thống tên miền (DNS) cho phép phân chia tên miền để quản lý và nó chia hệ thống tên miền thành zone và trong zone quản lý tên miền được phân chia đó. Các Zone chứa thông tin về miền cấp thấp hơn, có khả năng chia thành các zone cấp thấp hơn và phân quyền cho các DNS server khác để quản lý.

Ví dụ: Zone ".net" thì do DNS server quản lý zone ".net" chứa thông tin về các bản ghi có đuôi là ".net" và có khả năng chuyển quyền quản lý (delegate) các zone cấp thấp hơn cho các DNS khác quản lý như ".vnexpress.net" là vùng (zone) do vnexpress quản lý.

Hệ thống cơ sở dữ liệu của DNS là hệ thống dữ liệu phân tán hình cây như cấu trúc đó là cấu trúc logic trên mạng Internet [3].



Hình 1-3: Cấu trúc phân cấp DNS



Hình 1-4: DNS trong mô hình TCP/IP

DNS chủ yếu hoạt động trên giao thức UDP và cổng 53. Một số hoạt động khác có sử dụng giao thức TCP. Tại lớp vận chuyển, DNS sử dụng UDP hoặc TCP. UDP là giao thức không yêu cầu tính tin cậy của dữ liệu cao, thường được sử dụng cho việc trả lời các truy vấn (query) từ các host để đảm bảo tính nhanh chóng, khi sử dụng UDP thì hạn chế của gói tin là 512 bytes. Do đó UDP thường được sử dụng để trả lời các truy vấn của host. Còn TCP là giao thức đảm bảo thông tin, thường được sử dụng khi các DNS server cập nhật thông tin với nhau, đảm bảo tính chính xác. Thường thì khi các DNS server cập nhật thông tin với nhau, dữ liệu sẽ không bị hạn chế.

0 15	16 31
Transaction ID	Flags
Total Questions	Total Answer RRs
Total Authority RRs	Total Additional RRs
Questions	
Answer Resource Record structures	
Authority Resource Record structures	
Additional Resource Record structures	

Hình 1-5: Cấu trúc gói tin DNS

Trong các thành phần của cấu trúc gói tin DNS ở trên, khi đề cập đến vấn đề bảo mật, chúng ta chỉ quan tâm đến 4 vùng đó là:

a. Transaction ID : nó là một số ngẫu nhiên (random) dùng để so khớp với truy vấn phản hồi trở lại. Khi client nhận được một phản hồi (respone) từ server, nó sẽ kiểm tra xem số transaction ID này có trùng với số transaction ID mà nó đã gửi đi ban đầu hay không.

b. Answer Resource Record structures : đây là phần nội dung do DNS Server trả lời, được lấy trong resource record (RR) trên chính máy DNS Server đó.

c. Authority Resource Record structures : phần này chứa một trong 2 loại, hoặc là SOA hoặc là NS record chứa thông tin chứng nhận chủ nhân của RR(s) trong phần trả lời trên.

d. Additional Resource Record structures : phần này là thông tin resource record được thêm vào để gửi cho máy nhận (receiver)

Lưu ý: nếu có 2 phản hồi (responces), trình tự tiếp nhận của client sẽ diễn ra như sau: cái nào đến trước sẽ được chấp nhận trước, sau đó bỏ thông tin đã nhận trước đó khi nhận được cái sau. Đây thật sự là điểm yếu để tấn công đầu độc cache.

Tiêu chí để xác định xem những phản hồi (responces) có hợp lệ hay không đó là dựa trên các thông số ban đầu của các yêu cầu (requests) mà client đó đã gửi đi. Client chỉ chấp nhận những phản hồi với cùng một địa chỉ IP, số cổng (port number) và số transaction ID ban đầu do client đã gửi đi. Ví dụ theo bảng sau thì gói tin phản hồi sẽ được chấp nhận.

1.3. **CƠ CHẾ PHÂN GIẢI**

DNS service có 2 chức năng chính là phân giải tên thành IP và IP thành tên.

*1.3.1. **Phân giải tên thành địa chỉ IP:***

Root Name Server là máy chủ quản lý các name server ở mức top-level domain. Khi có query về 1 tên domain nào đó thì Root Name Server sẽ cung cấp tên và địa chỉ IP của name server quản lý top-level domain đó (thực tế thì hầu hết các root server cũng chính là máy chủ quản lý top-level domain) và đến lược các name server của top-level domain cung cấp danh sách các name server có quyền trên các secon-level domain mà domain này thuộc vào. Cứ như thế đến khi nào tìm được

máy chủ quản lý tên domain cần truy vấn.

Qua quá trình trên cho thấy vai trò rất quan trọng của Root Name Server trong quá trình phân giải tên domain. Nếu mọi Root Name Server trên mạng Internet không liên lạc được với nhau thì mọi yêu cầu phân giải tên đều sẽ không được thực hiện.

Ví dụ : khi người dùng truy cập tài nguyên mạng bằng tên miền hoặc host name (tên máy) ví dụ như truy cập vào trang web https://www.engisv.info bằng trình duyệt web, cái tên truy cập đó sẽ được phân giải thành địa chỉ IP, nếu tên miền và địa chỉ IP này được lưu cache lại trong bộ nhớ đệm thì máy tính người dùng không cần thiết phải liên hệ với máy DNS server liên tục để phân giải tên mà nó sẽ sử dụng dữ liệu được lưu này để trả ra kết quả cho người dùng. Nếu tên miền này chưa có trong cache trong bộ nhớ đệm, client sẽ liên hệ với DNS server đã được cấu hình ở phần khai báo địa chỉ IP của nó, nếu server này ở trạng thái sẵn sàng và nó không thể xác định được địa chỉ, client sẽ không hỏi thêm một server nào khác. Tuy nhiên, bởi vì DNS là hệ thống phân phối phân cấp, DNS server cục bộ sẽ cần liên hệ với những DNS server khác để có thể phân giải IP mà client yêu cầu.

DNS client được hiểu như là người có nhu cầu cần phân giải DNS. Bởi vì một một client hay một server đều cần sự phân giải địa chỉ tên miền và IP của DNS server để xác định được máy chủ dịch vụ mà chúng cần liên hệ, các client và các server đều có thể là DNS client.

Quá trình phân giải tên được thực hiện theo trình tự cụ thể sau:

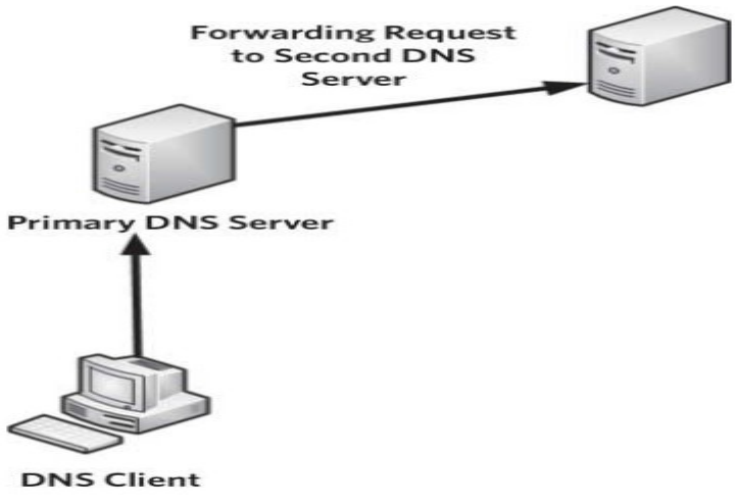
1. Client trên hệ thống mạng, cần phân giải www.engisv.info, client tra cứu file /etc/nsswitch.conf để biết thứ tự quá trình phân giải tên: **flies**, **nisplus**, **dns**
2. Client tra cứu file /etc/inet/hosts để tìm kiếm www.engisv.info, giả sử file không chứa thông tin cần truy vấn.
3. Client tạo 1 truy vấn đến NIS+ server để tra cứu thông tin về www.engisv.info, kết quả là không có record nào liên quan đến truy vấn.
4. Client tra cứu file /etc/resolv.conf để xác định danh sách tìm kiếm phân giải tên và địa chỉ DNS servers.

5. Client gửi yêu cầu truy vấn – recursive đến local DNS để tra cứu thông tin IP của www.google.com và client chờ cho đến khi quá trình phân giải tên hoàn thành.
6. Local DNS server tra cứu thông tin trong cache xem các thông tin truy vấn gần đây có record www.engisv.info đã được phân giải không. Nếu địa chỉ IP của www.engisv.info có sẵn trong cache, nó sẽ trả kết quả về cho client (non-authoritative).
7. Nếu Local DNS server không có thông tin về www.engisv.info, nó sẽ liên lạc với root servers và gửi một truy vấn dạng iterative: “Send me the best answer you have, and I will do all of the work.” (gửi cho tôi câu trả lời tốt nhất mà ta có và tôi sẽ làm tất cả công việc).
8. Root server trả về thông tin tốt nhất mà nó có bao gồm tên và địa chỉ của tất cả các server đang quản lý **.net** cùng với giá trị TTL cho biết những thông tin này sẽ được lưu bao lâu trong cache của local DNS server.
9. Local DNS server liên lạc với một trong những server quản lý .net thông qua kết quả từ root server trả về.
10. Máy server trong domain net trả về thông tin tốt nhất nó có, gồm tên và địa chỉ của tất cả các server của domain www.engisv.info và giá trị TTL.
11. Local DNS server liên lạc với một trong những server trong domain www.engisv.info và tạo một truy vấn tìm địa chị IP của www.engisv.info.
12. Server trong domain www.google.com trả về địa chỉ IP www.engisv.info, cùng với giá trị TTL.
13. Local DNS server trả về địa chỉ IP mà client yêu cầu.

Có 2 dạng truy vấn (query) trong DNS:

- **Truy vấn đệ quy (Recursive)**: Khi một DNS client truy vấn một DNS server, nó thực hiện một truy vấn đệ quy (***recursive query***). Trong khi có các yêu cầu từ các host, DNS server có thể trả lời các yêu cầu dữ liệu này hoặc trả lời tên miền không tồn tại. DNS server cũng có thể thực hiện các truy vấn đệ quy đến các máy chủ

DNS khác nếu nó được cấu hình chuyển tiếp yêu cầu đến DNS server khác khi nó không có câu trả lời.



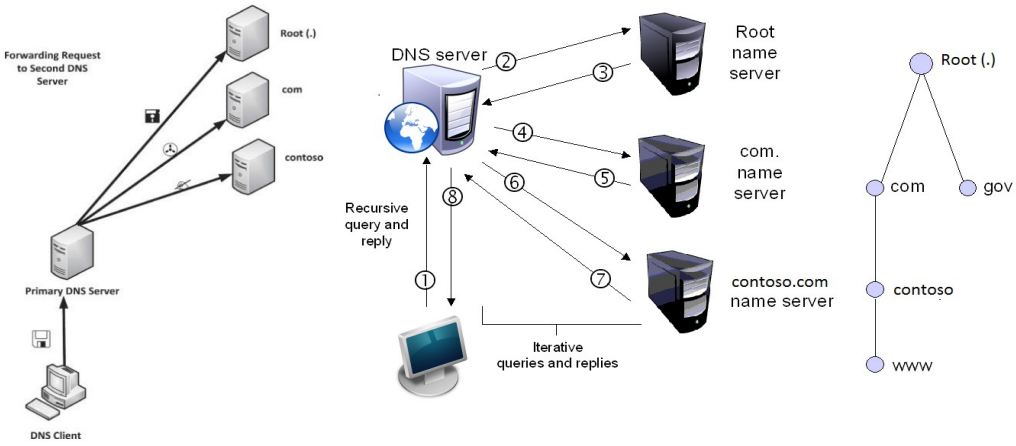
Hình 1-6: Truy vấn đệ quy

Khi DNS server nhận được yêu cầu, trước tiên nó sẽ kiểm tra có cache của mình xem có dữ liệu của yêu câu này hay không. Sau đó nó kiểm tra để xem nó có thẩm quyền hay không đối với yêu cầu domain. Nếu có biết câu trả lời và đủ thẩm quyền, nó sẽ hồi đáp với câu trả lời.

- Truy vấn lặp đi lặp lại (***iterative query***):

Nếu DNS server không biết câu trả lời và nó không được cấu hình chuyển tiếp yêu cầu đến một DNS server khác thì lúc này nó sẽ đóng vai trò là ***client DNS server*** và thay client thực hiện truy vấn, client DNS server sẽ sử dụng cơ chế phân cấp của DNS để tìm câu trả lời chính xác. Thay vì thực hiện truy vấn đệ quy, client DNS server sẽ thực hiện truy vấn lặp đi lặp lại (***iterative query***), với truy vấn này sẽ trả lại câu trả lời tốt nhất hiện nay nếu client DNS server không biết câu trả lời tốt nhất. Ví dụ như, khi user gõ ***www.contoso.com*** vào trình duyệt, client DNS server không có câu trả lời, client DNS server sẽ liên hệ với một root DNS server (.) để biết được địa chỉ của máy chủ tên miền ***com***. Sau khi nhận kết quả từ root DNS server (.), Client DNS server sau đó tiếp tục liên hệ với máy chủ tên miền ***com*** để lấy thông tin máy chủ tên của ***contoso.com***. Sau khi có thông tin từ contoso.com,

Client DNS server tiếp tục liên hệ với máy chủ tên miền của ***contoso.com*** để lấy địa chỉ IP của ***www.contoso.com***. Và sau cùng sau khi có được thông tin của ***www.contoso.com,*** Client DNS server trả lời cho client với địa chỉ IP đã phân giải. Ngoài ra, nó cũng thêm địa chỉ này vào cache của nó phục vụ cho các truy vấn sau này [9].



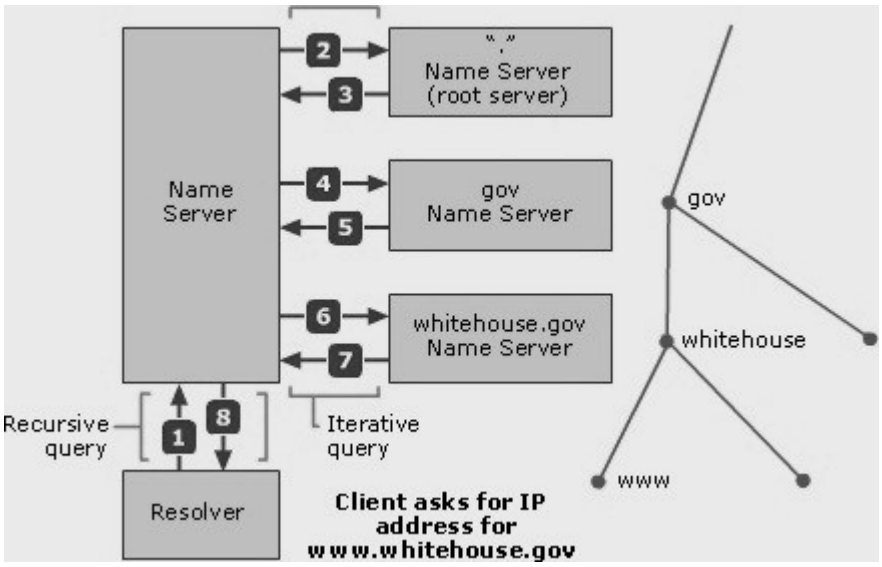
Hình 1-7: Truy vấn lặp lại

Trong một vài trường hợp, client DNS server không biết câu trả lời và nó không thể tìm thấy câu trả lời, client DNS server trả lời cho client rằng nó không thể tìm thấy hoặc là truy vấn domain không tồn tại.

Tóm lại việc truy vấn thường như sau:

- Truy vấn giữa Thiết bị truy vấn (host) ---> DNS Server là truy vấn đệ quy
- Truy vấn giữa DNS Server ---> DNS Server là truy vấn lặp lại.

Tức là khi client truy vấn đến DNS server nó sẽ dùng recursive, còn khi server truy vấn đến server khác, nó sẽ sử dụng iterative.



Hình 1-8: Client hỏi địa chỉ IP của www.whitehouse.gov

Hình trên cho ta thấy cả 2 truy vấn. Đầu tiên resolver hỏi nameserver xem có biết địa chỉ www.whitehouse.gov hay không. Nếu biết thì nameserver sẽ trả lại cho resolver một IP của domain name kia. Nếu ko biết, nameserver sẽ thực hiện các truy vấn lặp lại (2-7) hỏi các nameserver gần với domain name đó nhất để lấy cho được thông tin.

1.3.2. Phân giải địa chỉ IP thành tên host

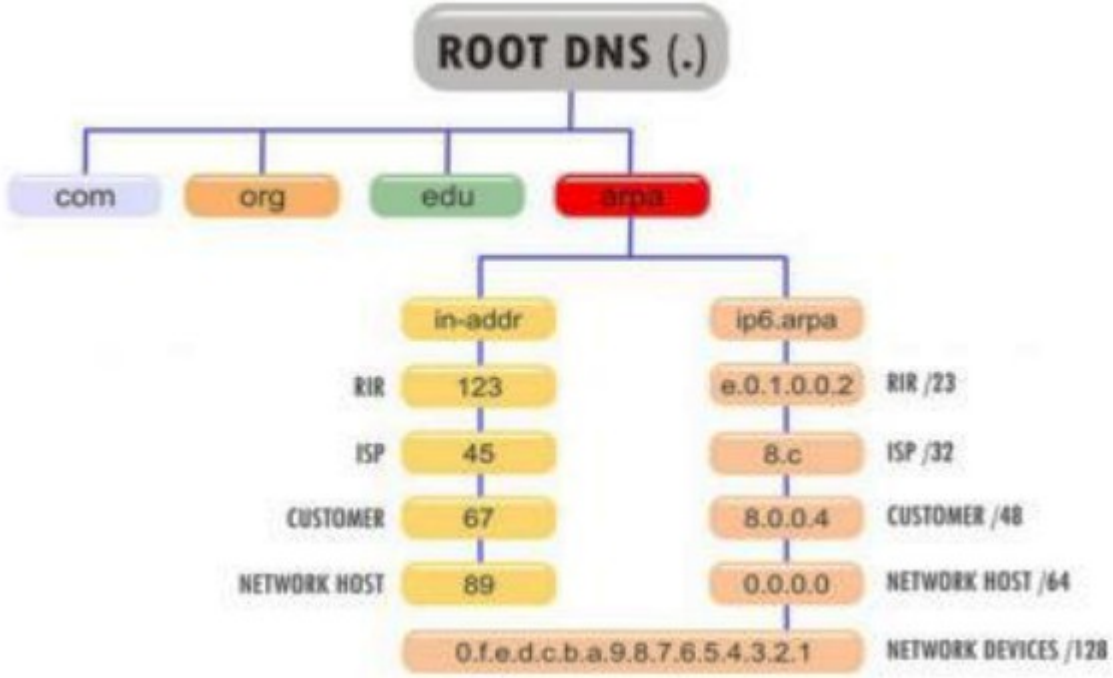
Ngoài chức năng chuyển đổi tên miền sang địa chỉ IP, hệ thống DNS còn có chức năng chuyển đổi ngược lại từ địa chỉ IP sang tên miền (reverse lookup). Chức năng reverse lookup cho phép tìm tên miền khi biết địa chỉ IP và được sử dụng trong trường hợp cần kiểm tra tính xác thực của các dịch vụ sử dụng trên Internet.

Ví dụ: Trong dịch vụ thư điện tử, thư điện tử (email) cần được chuyển qua một loạt các trạm chuyển tiếp thư điện tử (email exchanger) trước khi được chuyển đến người dùng. Khi email được chuyển từ một trạm chuyển tiếp thư điện tử này đến một trạm chuyển tiếp thư điện tử khác, trạm chuyển tiếp thư điện tử nhận thư sẽ dùng chức năng reverse lookup của hệ thống DNS để tìm tên miền của trạm chuyển tiếp thư điện tử chuyển thư đến. Trong trường hợp địa chỉ IP của trạm chuyển tiếp thư điện tử gửi không được khai báo bản ghi ngược, trạm chuyển tiếp thư điện tử nhận sẽ không chấp nhận kết nối này và sẽ loại bỏ thư điện tử. Không gian tên miền

các bản ghi ngược cũng được xây dựng theo cơ chế phân cấp như không gian tên miền của các bản ghi thuận:

Để có thể phân giải tên máy tính của 1 địa chỉ IP, trong không gian tên miền người ta bổ sung thêm 1 nhánh tên miền mà được lập chỉ mục theo địa chỉ IP. Phần không gian này có tên miền là in-addr.arpa.

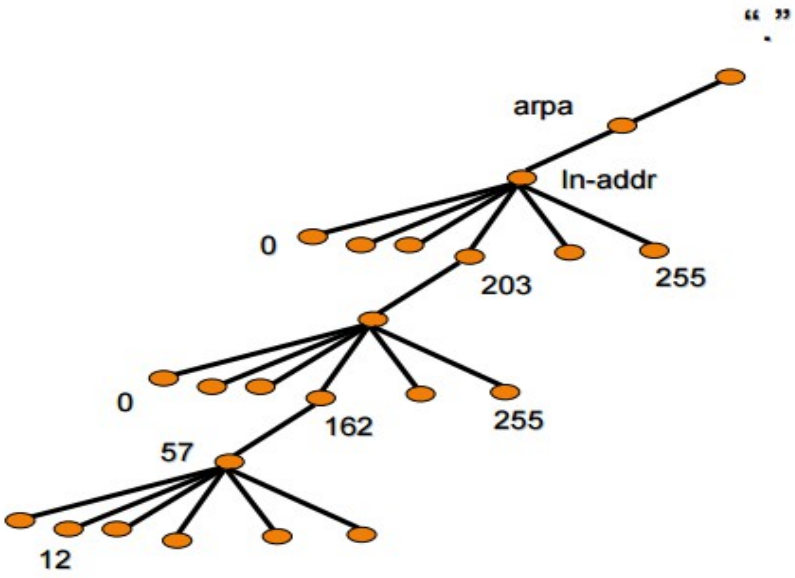
Mỗi node trong miền in-addr.arpa có một tên nhãn là chỉ số thập phân của địa chỉ IP. Ví dụ miền in-addr.arpa có thể có 256 subdomain tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi subdomain lại có 256 subdomain con nữa ứng với byte thứ 2. Cứ như thế và đến byte thứ 4 có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ IP tương ứng.



Hình 1-9: Cấu trúc không gian tên miền ngược của IPv4, IPv6 trong cây tên miền chung

Đối với thế hệ địa chỉ IPv4, cấu trúc của tên miền ngược có dạng như sau: www.zzz.yyy.xxx.inaddr. arpa. Trong đó: xxx, yyy, zzz, www là các số viết trong hệ thập phân biểu diễn giá trị của 4byte cấu thành 1 địa chỉ IPv4. Ví dụ: Một máy tính trên mạng được gán địa chỉ IPv4 203.162.57.101 thì tên miền ngược tương ứng sẽ là 101.57.162.203.in-addr. arpa. Máy chủ có tên miền: mail.vnnic.net.vn Ánh xạ

vào tên miền thuận bằng bản ghi PTR: 12.57.162.203.in-addr.arpa. IN PTR mail.vnnic.net.vn



Hình 1-10: Hình vẽ minh họa cấu trúc tên miền ngược trong IPv4

Đối với thế hệ địa chỉ Internet mới IPv6, cấu trúc tên miền ngược có khác một chút. Cụ thể: Không gian các tên miền ngược của các địa chỉ IPv6 không nằm dưới miền in-addr.arpa như của IPv4 mà nằm dưới miền .ip6.arpa. Do hoàn toàn không còn khái niệm class (lớp) trong IPv6 và một địa chỉ IPv6 được biểu diễn dưới dạng số hexa nên cấu trúc phân cấp tên miền ngược trong IPv6 cũng không chia theo lớp như ở IPv4 mà được phân cấp theo từng biên 4 bit tương ứng với mỗi số hexa cấu thành nên một địa chỉ IPv6 arpa In-addr 0 255 12 57 0 162 255 203 “.”. Ví dụ: Một node mạng được gán địa chỉ IPv6 2001:0dc8:0123:1234:abcd:0000:0000:0000 thì tên miền ngược tưng ứng sẽ là:

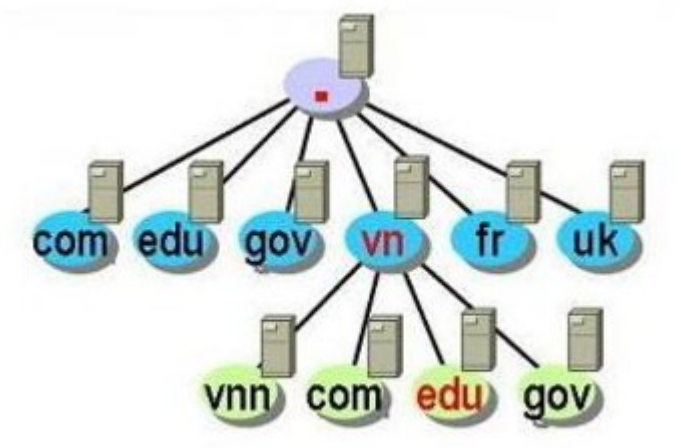
0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.4.3.2.1.3.2.1.0.8.c.d.0.1.0.0.2.ip6.arpa

1.3.3. Chức năng của hệ thống tên miền DNS (Domain Name System)

Mỗi Website có một tên (là tên miền hay đường dẫn URL: Uniform Resource Locator) 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).

Hệ thống tên miền giúp cho nó có thể chỉ định tên miền cho các nhóm người sử dụng Internet trong một cách có ý nghĩa, độc lập với mỗi địa điểm của người sử dụng. Do đó, World Wide Web siêu liên kết và trao đổi thông tin trên Internet có thể duy trì ổn định và cố định ngay cả khi định tuyến dòng Internet thay đổi hoặc những người tham gia sử dụng một thiết bị di động. Tên miền internet dễ nhớ hơn các địa chỉ IP như là 208.77.188.166 (IPv4) hoặc 2001: db8: 1f70:: 999: de8: 7648:6 e8 (IPv6).



Hình 1-11: Địa chỉ IP được dịch thành các tên miền

Mọi người tận dụng lợi thế này khi họ thuật lại có nghĩa các URL và địa chỉ email mà không cần phải biết làm thế nào các máy sẽ thực sự tìm ra chúng. Hệ thống tên miền phân phối trách nhiệm gán tên miền và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền. Những máy chủ có tên thẩm quyền được phân công chịu trách nhiệm đối với tên miền riêng của họ và lần lượt có thể chỉ định tên máy chủ khác độc quyền của họ cho các tên miền phụ. Kỹ thuật này đã thực hiện các cơ chế phân phối DNS, chịu đựng lỗi, và giúp tránh sự cần thiết cho một trung tâm đơn lẻ để đăng kí được tư vấn và liên tục cập nhật.

Nói cách khác, DNS trợ giúp qua lại với nhau để dịch địa chỉ IP thành tên và ngược lại chứ không có chức năng nhớ IP. DNS chỉ định tên miền cho các nhóm người sử dụng internet theo một cách có ý nghĩa, độc lập với mỗi địa điểm của người sử dụng. WWW duy trì tính ổn định khi dòng internet thay đổi. Hệ thống tên miền phân phối trách nhiệm gán tên và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền. Từ đó tăng khả năng chịu đựng lỗi và tránh việc quá tải.

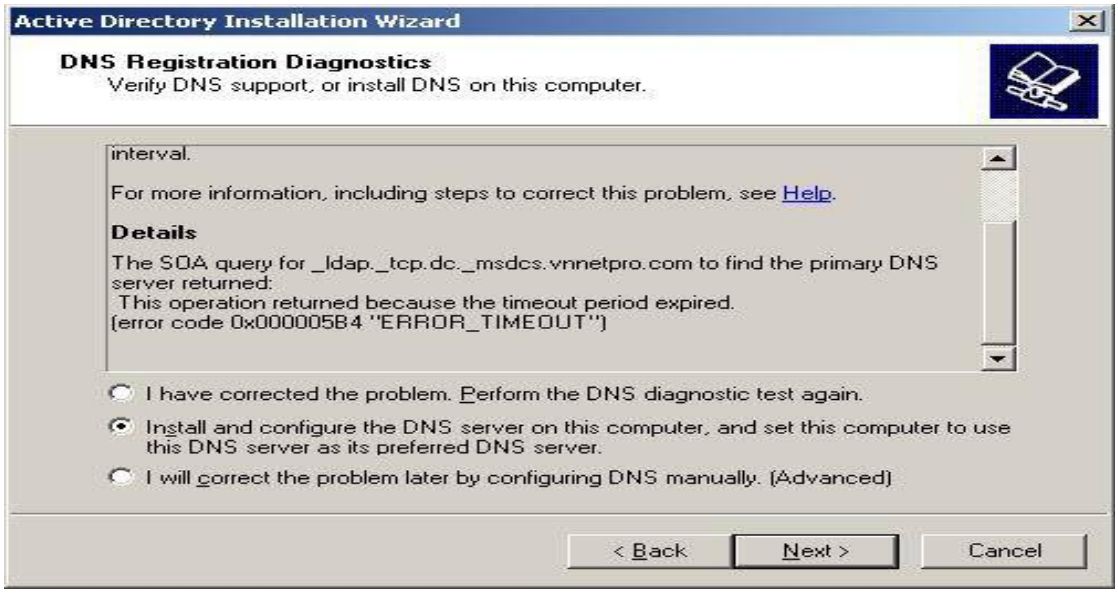
1.1.1. ***Một số khái niệm cơ bản trong DNS:***

+ **Domain Name và Zone**:

Một domain có thể có 1 hoặc nhiều domain con bên trong nó gọi là subdomain.

Ví dụ : domain com có nhiều domain con như vnnetpro.com, google.com,…

Bạn có thể delegation control cho các DNS Server khác quản lý. Những domain và subdomain mà DNS Server quản lý gọi là Zone. Như vậy 1 zone có thể gồm 1 domain, 1 hoặc nhiều subdomain [5].



Hình 1-12: Zone và Domain

Các loại zone :

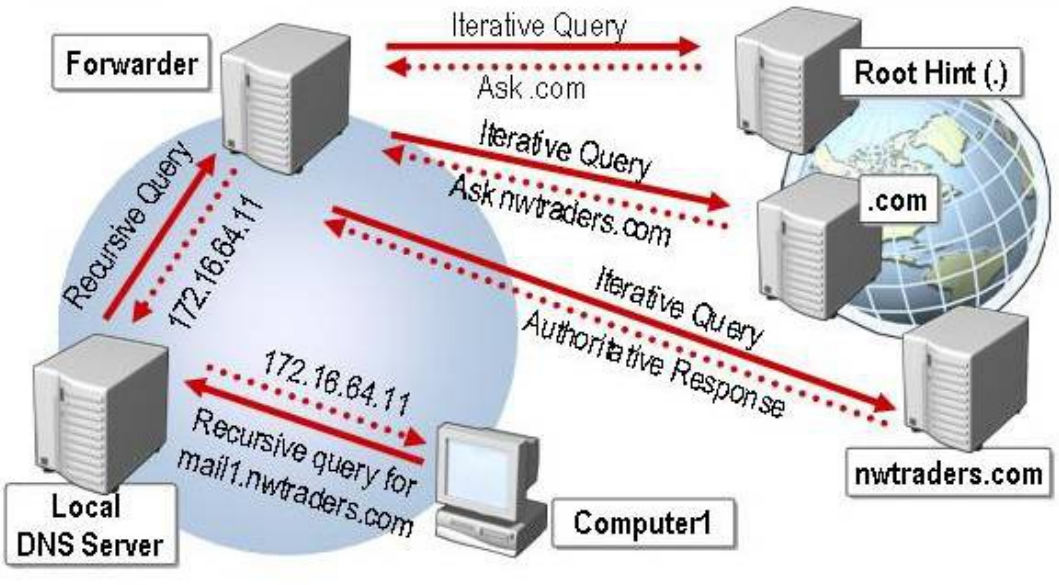
- Primary zone : cho phép đọc và ghi cơ sở dữ liệu
- Secondary zone : là bản sao cơ sở dữ liệu DNS của Primary zone, có được nhờ quá trình zone transfer (phải được primary zone cho phép transfer).
- Stub zone : chứa bản sao cơ sở dữ liệu DNS của zone nào đó, nó chỉ chứa 1 vài resource record.

+ Delegation:

Một trong các mục tiêu khi thiết kế hệ thống DNS là khả năng quản lý phân tán thông qua cơ chế ủy quyền (delegation control). Trong 1 domain có thể tổ chức thành nhiều subdomain, mỗi subdomain có thể được ủy quyền cho 1 tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong subdomain này. Khi đó parent domain chỉ cần 1 con trỏ, trỏ đến subdomain này khi có truy vấn đến subdomain đó [5].

+ Forwarder:

Là kỹ thuật cho phép DNS Server local chuyển yêu cầu truy vấn cho các DNS Server khác để phân giải các domain bên ngoài.



Hình 1-13: Forwarder DNS queries

Theo mô hình trên thì ta thấy khi lnternal DNS server nhận yêu cầu truy vấn của Computer1, thì nó sẽ kiểm tra xem có thể phân giải được tên miền này hay không, nếu không phân giải được thì nó sẽ chuyển yêu cầu này lên Forwarder DNS Server (multihomed) để nhờ Name Server này phân giải dùm. Sau khi xem xét xong thì Forwarder DNS Server sẽ trả lời yêu cầu này cho Internal DNS Server hoặc nó sẽ tiếp tục forwarder lên các Name Server khác ngoài Internet.

+ Stub Zone:

Là zone chứa bản sao cơ sở dữ liệu DNS từ Master Name Server. Stub zone chỉ chứa các resource record cần thiết như : A, SOA, NS, 1 hoặc vài địa chỉ của Master Name Server hỗ trợ cơ chế cập nhật Stub zone, cơ chế chứng thực Name Server trong zone và cung cấp cơ chế phân giải tên domain được hiệu quả hơn, đơn giản hóa công tác quản trị.

+ Resolver:

Resolver là những Client truy vấn Name Server. Bất kỳ máy tính nào cần truy vấn thông tin về Domain Name đều dùng Resolver. Resolver đảm nhận 3 vai trò sau :

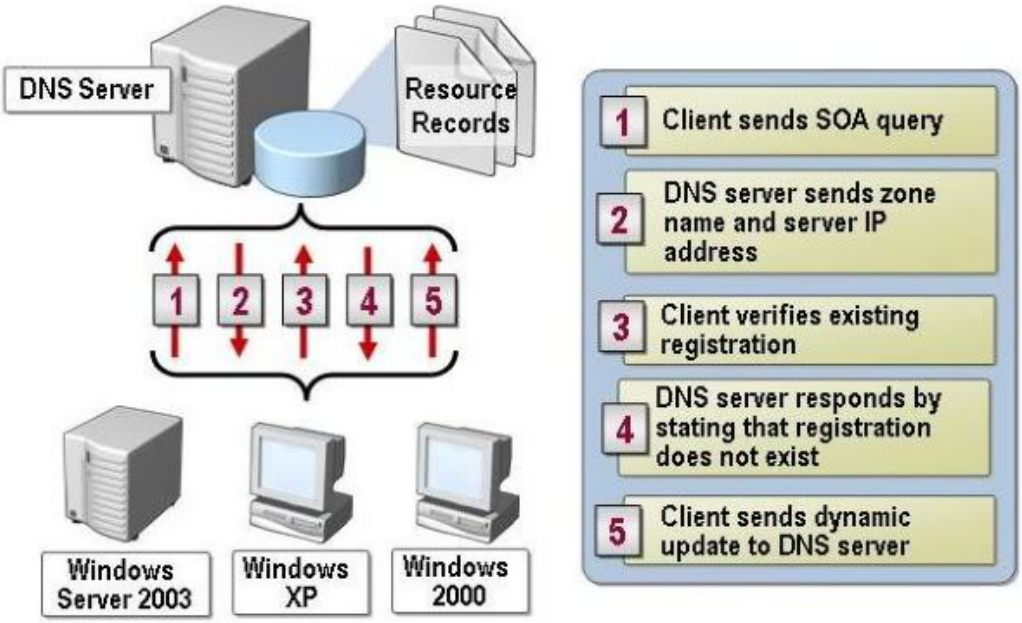
- Querying a Name Server : truy vấn 1 Name Server.
- Interpreting Responses : phân giải kết quả.
- Returning the information to the programs that requested it : trả kết quả về cho chương trình đã yêu cầu.

+ Dynamic DNS

Dynamic DNS là phương thức ánh xạ tên miền --> địa chỉ IP có tần suất thay đổi cao, dynamic DNS cung cấp 1 chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ dynamic DNS gọi là dynamic DNS Client. Chương trình này giám sát sự thay đổi địa chỉ IP tại host và liên hệ với hệ thống DNS mỗi khi địa chỉ IP của host thay đổi và sau đó update thông tin vào cơ sở dữ liệu DNS về sự thay đổi địa chỉ đó.

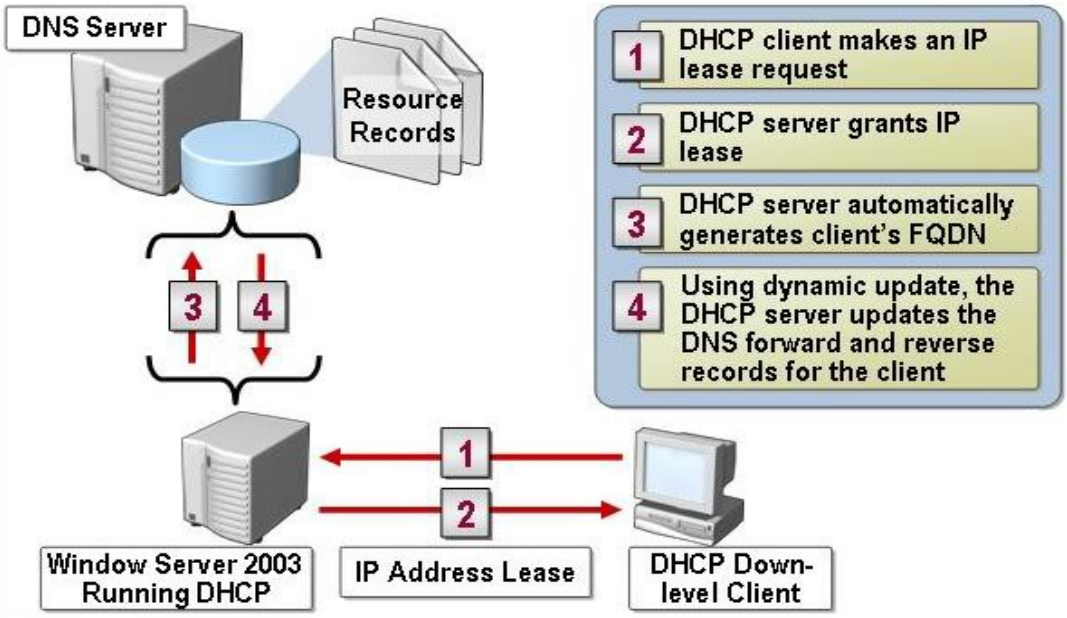
DNS Client đăng ký và cập nhật resource record của nó bằng cách gửi dynamic

update.

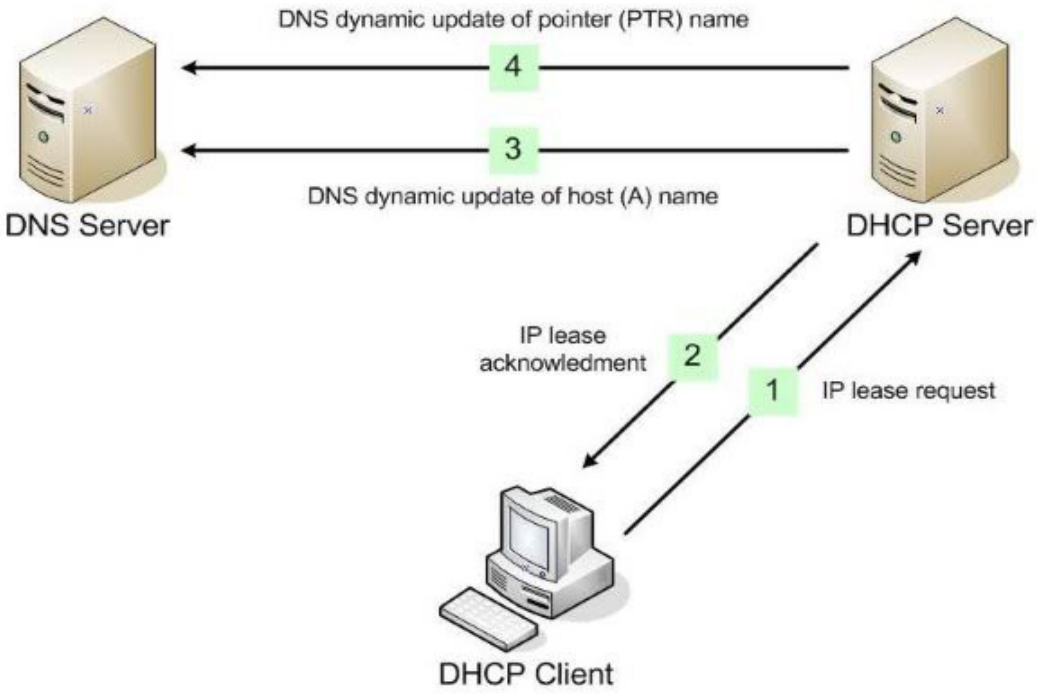


Hình 1-14: Dynamic update

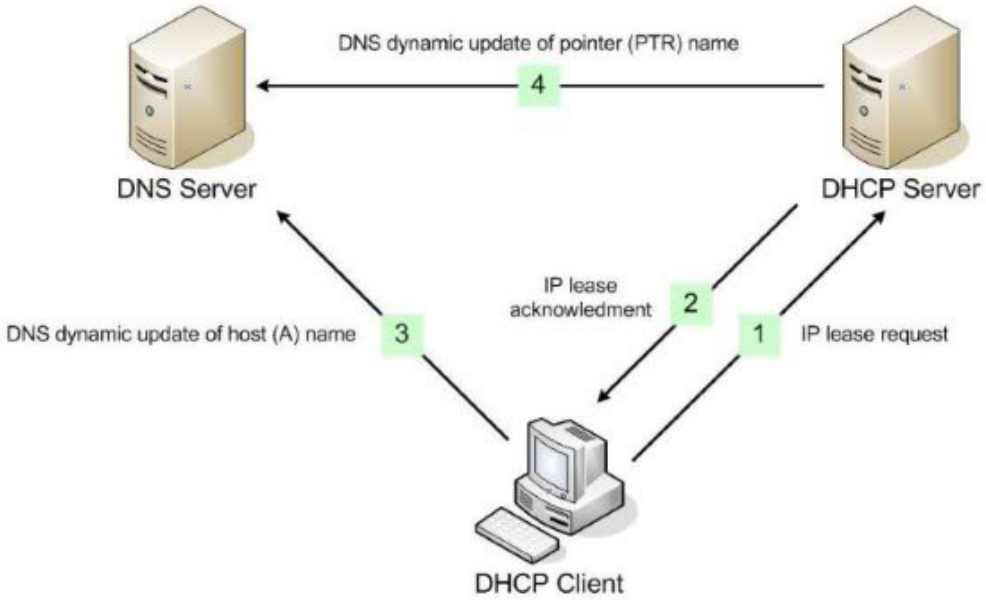
Các DHCP Server đăng ký và cập nhật resource record cho client



Hình 1-15: DHCP Server cập nhật Dynamic update



Hình 1-16: DHCP & DNS Interaction for pre-Windows 2000 Clients



Hình 1-17: DHCP and DNS Interaction

+ Caching:

DNS Server và Client sẽ lưu lại những truy vấn (caching) để khi được truy vấn lần sau nó sẽ tìm trong cache trước, nếu cache có nó sẽ trả lời ngay lập tức mà không cần truy vấn nữa. Đều này giúp cho mạng hoạt động nhanh hơn (tăng performing).

+ Time to live (TTL):

Những dữ liệu được cache lại trong DNS server hoặc Client sẽ không tồn tại vĩnh viễn vì có thể thông tin của dữ liệu đó thực tế đã bị thay đổi bởi Primary Name Server phụ trách cho dữ liệu đó. TTL là thời gian mà các DNS Server hoặc Client được phép cache thông tin đã truy vấn được, sau thời gian đó các DNS Server hoặc Client sẽ phải hủy tất cả các cache đó và đi lấy thông tin mới bằng cách truy vấn lại. Giá trị TTL này có thể được thay đổi bởi người quản trị trong việc khai báo TTL cho dữ liệu đó.

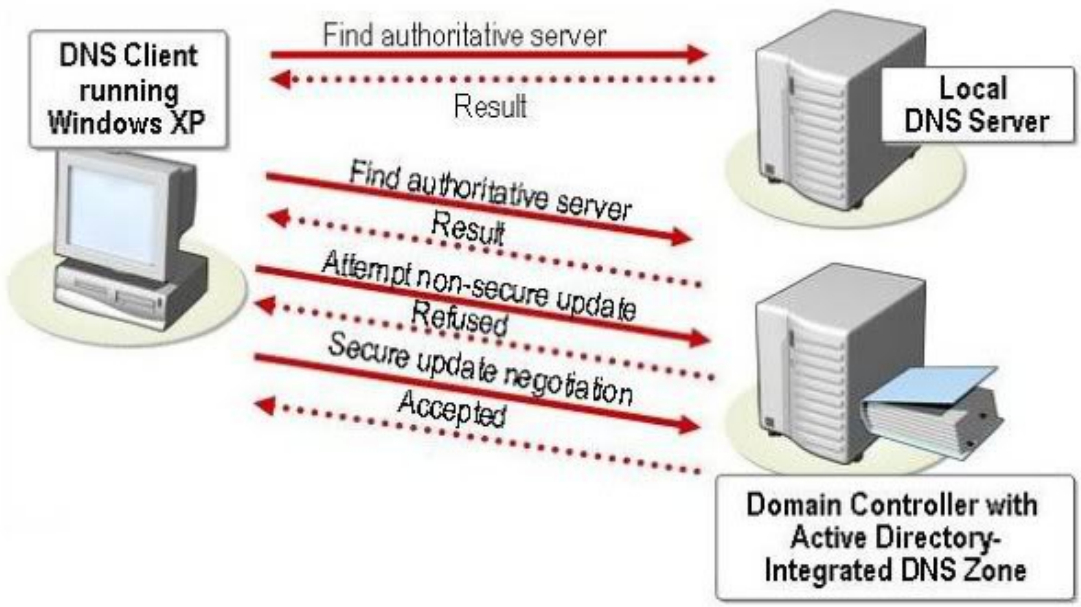
+ Active Directory – Intergrated Zone:

Sử dụng Active Directory – Intergrated Zone có 1 số thuận lợi sau :

- Security : cơ sở dữ liệu DNS được tích hợp chung với Active Directory nên không còn ở dạng plaintext khi transfer nữa mà được encypt chung với cơ sở dữ liệu của AD.
- Replicate : sử dụng cơ chế replicate của AD để update và replicate DNS database
- Sử dụng Security Dynamic update
- Sử dụng nhiều Master Name Server để quản lý Domain Name thay vì chỉ sử dụng 1 Master Name Server

Mô hình Active Directory – Intergrated zone sử dụng Security Dynamic

Update



Hình 1-18: Secure Dynamic Update

***Kết luận chương 1*:** Nội dung chương 1 cho ta một cái nhìn tổng quan về hệ thống DNS, chức năng, cơ chế phân giải và cấu trúc gói tin, các bản ghi, một số khái niệm cơ bản trong DNS. Từ đó thấy được tầm quan trọng của hệ thống DNS đối với internet. DNS đang là một đối tượng bị tấn công nhiều nhất hiện nay.

CHƯƠNG 2. PHÂN TÍCH CÁC CÁCH THỨC TẤN CÔNG VÀO DNS

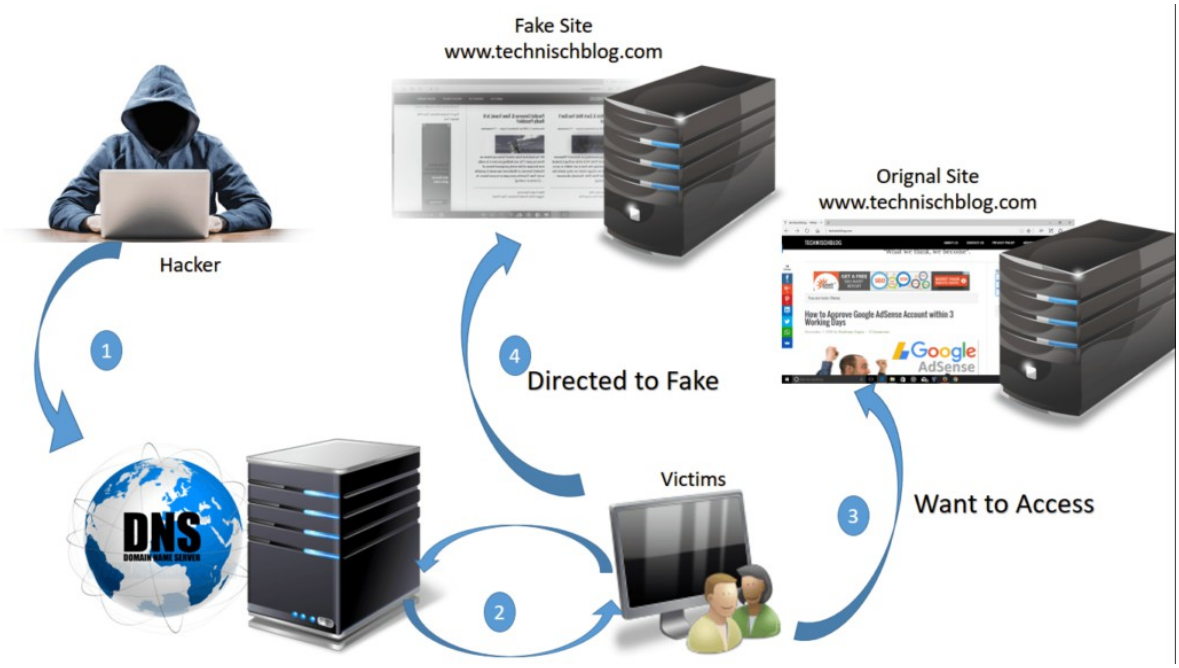
2.1: CÁC LỖ HỔNG CỦA DNS:

Hệ thống DNS thực chất là một tập hợp hệ thống phần cứng và các công cụ phần mềm phục vụ cho nhiệm vụ phân giải tên miền.

Ngoài các hệ thống phần cứng và các công cụ phần mềm chạy dưới dạng dịch vụ thì cần có các giao thức DNS (Bao gồm định dạng gói tin, giao thức truyền, …) để có thể tiến hành trao đổi thông tin giữa máy client với các máy chủ DNS và giữa các máy chủ DNS với nhau.

Chính vì DNS hội tụ đầy đủ các yếu tố: Phần cứng, phần mềm và giao thức như đã trình bày ở trên nên hệ thống DNS luôn luôn tiềm ẩn các lỗ hổng mà hacker có thể sử dụng để khai thác và làm chủ hệ thống, từ đó gây ra các ảnh hưởng tới người dùng.

Do một client bình thường tin tưởng các thông tin phân giải do DNS Server cung cấp. Do đó, nếu DNS Server bị tấn công vì mục đích nào đó nhằm thay đổi các thông tin phân giải trả về cho client. Điều này thật nguy hiểm cho client khi nhận được những thông tin phân giải đã bị "nhiễm bẩn".



Hình 2-19: Attacker tấn công DNS đánh lạc hướng người dùng

Nhiều hệ thống DNS đang hoạt động chấp nhận xử lý đồng thời nhiều yêu cầu truy vấn (query) của một tên miền duy nhất, đặc điểm này cho phép tin tặc dễ dàng tấn công vào các DNS server có chức năng hỏi hộ (recursive) và lưu giữ kết quả (caching) với mục đích làm thay đổi ánh xạ tên miền và hướng người dùng đến một địa chỉ IP bất hợp lệ tuỳ ý.

2.1.1. Mục đích tấn công hệ thống DNS:

Khi tấn công hệ thống DNS, attacker mong muốn thực hiện một số hành vi:

- Lừa người sử dụng truy cập tới các website giả mạo do attacker lập ra để thực hiện các hành vi lừa đảo, ăn cắp mật khẩu, thông tin đăng nhập, cài cắm các phần mềm độc hại. Các thông tin này có thể vô cùng quan trọng: tài khoản ngân hàng, tài khoản quản trị, …
- Tăng traffic cho website: attacker chuyển hướng người dùng khi họ truy cập các website phổ biến về địa chỉ website mà attacker muốn tăng traffic. Mỗi khi người dùng truy cập một trong các website kia thì trả về địa chỉ IP website mà attacker mong muốn, qua đó làm tăng traffic cho website.
- Gián đoạn dịch vụ: mục đích này nhằm ngăn chặn người dùng sử dụng một dịch vụ của một nhà cung cấp nào đó.

2.1.2. Đối tượng để Attacker tấn công:

- Đối tượng tin tặc nhắm đến là các DNS server có các đặc điểm sau đây:

Phục vụ nhiều người dùng.

Có chức năng hỏi hộ (recursive) và lưu giữ kết quả (caching).

Có điểm yếu: chấp nhận xử lý đồng thời nhiều yêu cầu truy vấn (query) của một tên miền duy nhất.

Sử dụng 1 port nguồn (UDP hay TCP) cố định và duy nhất cho tất cả các request.

(Tuỳ chọn) không kiểm tra chặt chẽ tính chính xác và logic của phần thông tin thêm (addition records) trong các DNS reply trả về.

- DNS luôn có nguy cơ tiềm ẩn khi hệ thống không sử dụng DNS tách rời.

Bước đầu tiên của kẻ tấn công là tìm một server DNS có thể truy cập từ bên ngoài cho công ty này và các dữ liệu thuộc miền DNS có sử dụng chức năng zone transfer.

Dựa vào các thông tin này, kẻ tấn công có thể tạo ra một bản đồ hoàn chỉnh cho hệ thống mạng của công ty. Nếu một trong các server của họ đã có hai địa chỉ IP, và một server là địa chỉ công cộng thì điều này có nghĩa là server này đồng thời kết nối với hệ thống mạng nội bộ và internet mà không có bức tường lửa bảo vệ.

Kẻ tấn công chỉ việc kết nối vào server này để đi qua bức tường lửa và để khám phá nguy cơ bị xâm nhập của server để có thể nắm quyền kiểm soát. Sau đó sử dụng server đó để vào hệ thống mạng. Trong thời gian ngắn đã có thể kiểm soát được hoàn toàn Doman Admin.

- Lỗ hổng bảo mật xuất hiện trong quá trình truyền thông tin từ Primary DNS và Secondary DNS.

Nếu không thiết lập đường truyền cho quá trình truyền dữ liệu "zone transfer" giữa Primary DNS và Secondary DNS bằng một đường truyền riêng trong hệ thống hoặc từ site to site không có kênh VPN riêng và thông tin được truyền đi không được mã hoá cũng chính là tạo kẽ hở cho hacker tấn công.

- Một số server cuối của hệ thống nội bộ có thể truy cập trực tiếp từ mạng internet. Khi kẻ tấn công áp dụng zone transfer để xác định tên và địa chỉ IP cho hàng trăm máy tính của một hệ thống. Nghiên cứu kỹ các tên được mô tả sẽ xác định được một số server cuối của hệ thống nội bộ có thể truy cập trực tiếp từ mạng internet. Rõ ràng đây là một lỗ hổng trong chế độ bảo mật của hệ thống đó.

2.2. CÁC CÁCH THỨC TẤN CÔNG VÀO HỆ THỐNG DNS.

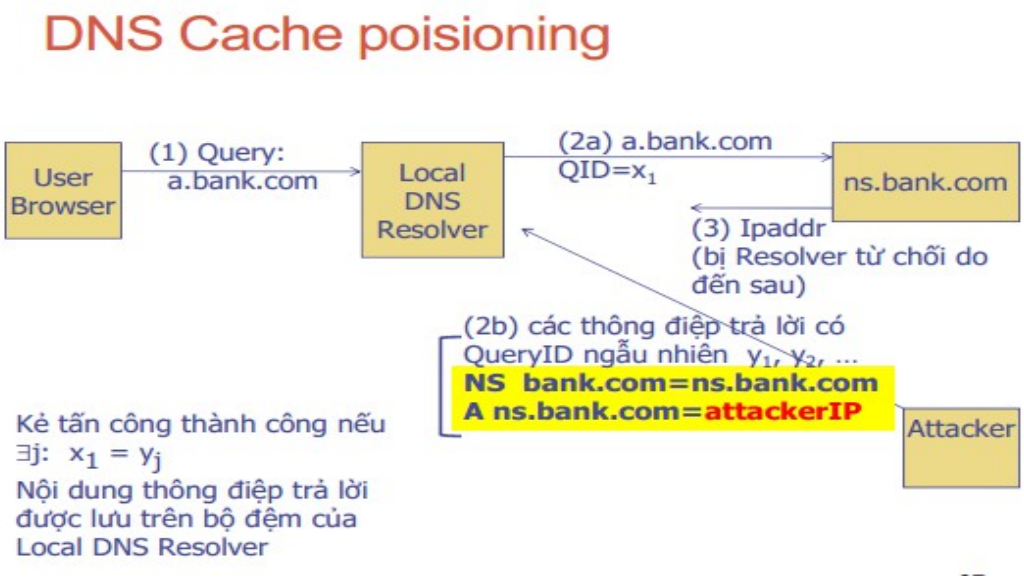
2.2.1. Tấn công đầu độc cache (cache poisoning attack):

Đây là một phương pháp tấn công máy tính nhờ đó mà dữ liệu được thêm vào hệ thống cache của các DNS server. Từ đó, các địa chỉ IP sai (thường là các địa chỉ IP do attacker chỉ định) được trả về cho các truy vấn tên miền nhằm chuyển hướng người dùng tư một website này sang một website khác.

Để khai thác theo hướng này, attacker lợi dụng lỗ hổng của phần mềm DNS, do các DNS responses không được xác nhận để đảm bảo chúng được gửi từ các server được xác thực, các bản ghi không đúng đắn sẽ được cache lại và phục vụ cho các user khác.

Ví dụ: Attacker thay thế địa chỉ IP cho một bản ghi DNS trên DNS server thành địa chỉ IP của server mà attacker đang có quyền điều khiển. Trên server này, attacker có triển khai một số phần mềm mã độc để khi người dùng bị chuyển qua sẽ dễ dàng bị nhiễm mã độc.

Như đã đề cập trong phần lý thuyết bên trên, các DNS Server sau khi trả thông tin đã phân giải được vào cache (cache trên DNS Server), mục đích là để tối ưu cho việc phân giải lần sau. Lợi dụng cơ chế này, các attacker tiến hành đầu độc cache của DNS Server.



Hình 2-20: DNS cache poisoning

Một bộ nhớ đệm DNS có thể bị nhiễm độc nếu nó chứa một mục nhập (entry) không chính xác. Ví dụ, nếu một kẻ tấn công được quyền kiểm soát một máy chủ DNS và thay đổi một số thông tin trên đó, ví dụ, địa chỉ google.com sẽ bị chuyển đến địa chỉ IP mà kẻ tấn công sở hữu trong khi người dùng không hề hay biết, khi đó máy chủ DNS sẽ khiến người dùng Google.com để tìm kiếm đi đến sai địa chỉ. Mà địa chỉ đó của kẻ tấn công thì có thể chứa một số loại trang web lừa đảo độc hại.

Hình 2-21: Một trang web giả mạo Vietcombank

Sự nhiễm độc DNS như thế này hoàn toàn có thể lây lan. Ví dụ, các nhà cung cấp dịch vụ Internet khác nhau có thể nhận được thông tin DNS của họ từ các máy chủ đã bị xâm nhập, các entry DNS chứa mã độc sẽ lây lan sang các nhà cung cấp dịch vụ Internet và được lưu trữ ở đó. Sau đó nó sẽ tiếp tục lây lan sang các bộ định tuyến gia đình ta và bộ nhớ đệm DNS địa phương trên máy tính dẫn đến việc tìm kiếm các entry DNS nhận được phản hồi không chính xác mà người dùng hoàn toàn không hề hay biết.

Có vài cách để thực hiện việc này:

- Cách thứ nhất: thiết lập một DNS Server giả mạo với các record độc hại.

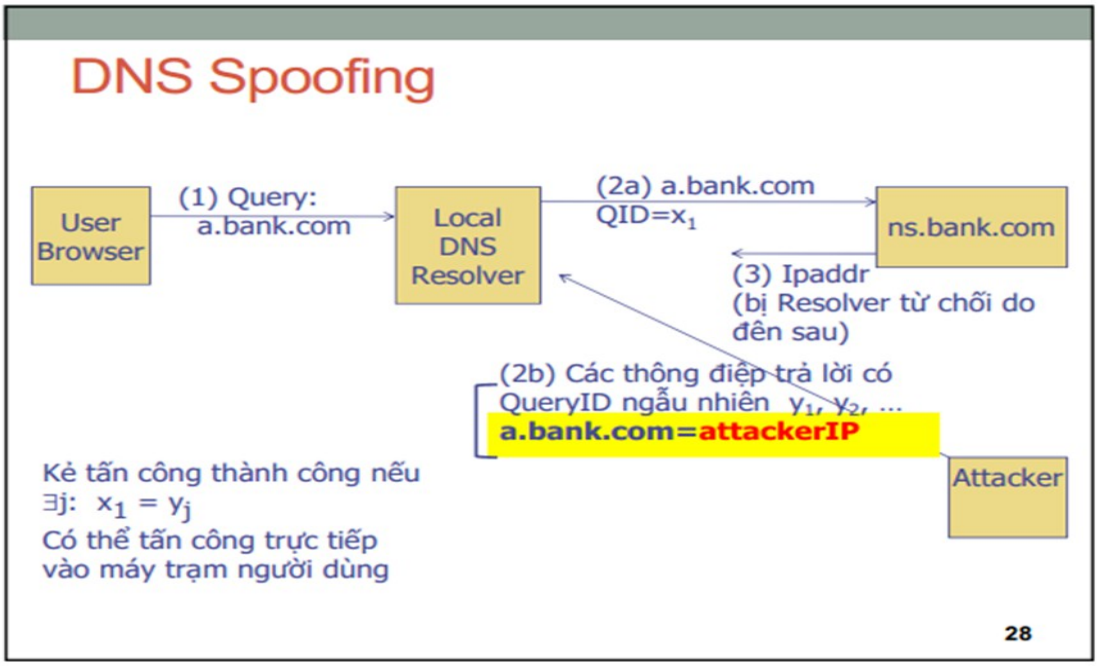
Mục đích của kẻ tấn công là muốn dẫn các client khi phân giải một cái tên nào đó về địa chỉ IP giả mạo, ví dụ khi client cần phân giải địa chỉ www.cnn.com thì được trả về địa chỉ IP giả là 66.66.66.66. Khi nào record giả còn tồn tại trong cache của DNS Server nạn nhân, các truy vấn của www.cnn.com sẽ được chuyển hướng đến 66.66.66.66, đây có thể là một máy tính được đặt dưới sự kiểm soát của attacker, các thông tin đến www.cnn.com sẽ được attacker forward đến đối tượng thật sự www.cnn.com và ngược lại. Do đó client cuối cùng không biết có sự tồn tại của máy "man in the middle".

- Cách thứ 2: Gửi một spoofed reply đến client nạn nhân thông qua sự giúp đỡ của 1 sniffer.

Thay vì thiết lập một DNS Server giả mạo, nếu attacker có thể đặt mình vào vị trí giữa client và DNS Server, attacker có thể ngăn chặn các request của client gửi đến DNS Server và sau đó gửi gói tin reply với thông tin sai đến client.

Xin nhắc lại là client chỉ chấp nhận các gói tin reply với cùng các thông số đã gửi đi ban đầu như Transaction ID, địa chỉ IP và số port. Để biết các thông số này, attacker có thể nghe lén để capture lại các gói tin trong mạng. Sau khi đã có các thông số đầy đủ, attacker có thể tạo gói tin reply DNS giả để gửi đến cho client. Nội dung gói tin chứa thông tin sai trái phục vụ cho mục đích đen tối của attacker.

Tuy nhiên hạn chế của phương pháp này là gói tin reply phải của attacker phải đến trước gói tin hợp lệ của DNS Server. Nếu gói tin hợp lệ của DNS Server đến trước thì cách tấn công này sẽ không thực hiện được. Đó là do client chỉ chấp nhận gói tin reply nào hợp lệ đến trước, và sẽ làm ngơ (ignore) các gói tin đến sau.
Có nhiều cách để thực hiện ý đồ này của attacker, và để tăng khả năng thành công của phương pháp này, attacker có thể tiến hành tấn công từ chối dịch vụ (DOS) để làm chậm hoạt động của DNS Server. Do phải capture các gói tin để lấy các thông số của gói tin request DNS, việc capture các gói tin này khó có thể thực hiện trong môi trường mạng switch (switched network). Do đó, kỹ thuật tấn công ARP spoofing phải được thực hiện trước.
- Cách thứ 3: gửi một lượng lớn spoofing reply đến client nạn nhân



Hình 2-22: DNS spoofing

Kỹ thuật tấn công dựa vào số ID DNS spoofing đòi hỏi kẻ tấn công phải biết chính xác số ID giao dịch giữa client và server. Điều này có thể được thực hiện bằng cách gửi một lượng rất lớn các gói tin reply chứa số Transaction ID khác nhau đến client, hi vọng một trong số các gói tin gửi đến client sẽ hợp lệ.

Trên thực tế, số ID này chỉ chiếm 2 byte bộ nhớ, cho nên nó chỉ có tất cả 65525 trường hợp. Vì vậy, bằng cách gửi 65525 gói tin reply (mỗi gói tin có số ID khác nhau), một trong số chúng chắc chắn sẽ phù hợp với số Transaction ID giao dịch giữa client và server, đồng thời có thể làm ngập lụt (fool) máy nạn nhân.

Với cách tấn công này, attacker không cần phải nghe lén số Transaction ID giao dịch giữa client và server. Nhưng vấn đề của nó là khi nào thì nên tiến hành thực hiện tấn công? Đó là, làm thế nào để biết khi nào client thực hiện truy vấn DNS? Đây là việc gây khó khăn cho phương thức tấn công này.

- Cách thứ 4: attacker gửi một lượng lớn spoofing reply đến DNS Server

Trong cách thứ 3, attacker không thể biết khi nào client thực hiện một truy vấn. Tuy nhiên, trong thực tế, attacker có thể tự thực hiện truy vấn và sau đó gửi gói tin reply giả mạo đến DNS Server. Sau đó, DNS Server sẽ chứa thông tin bị đầu độc.

Trở ngại của phương pháp này đó là gói tin reply phải chứa cùng số Transaction ID và số port mà DNS Server victim đã sử dụng. Để giải quyết vấn đề này, đối với số Transaction ID thì attacker sử dụng phương pháp birthday attack. Trên DNS Server thì source port sử dụng hầu như không đổi đối với từng client. Lợi dụng điều này, đầu tiên attacker yêu cầu DNS Server victim phân giải một địa chỉ tên domain nào đó của attacker. Trên máy này, sau khi nhận được truy vấn attacker có thể biết được source port nào đang được sử dụng trên DNS Server victim. Dựa trên sự tính toán này, cùng với số source port đã biết, attacker thực hiện gửi 650 request và 650 reply giả mạo đến DNS Server victim. Xác suất thành công của phương pháp tấn công này đạt khoản 96% tỉ lệ thành công.

2.2.2. Tấn công khuếch đại DNS (DNS Amplification Attack):

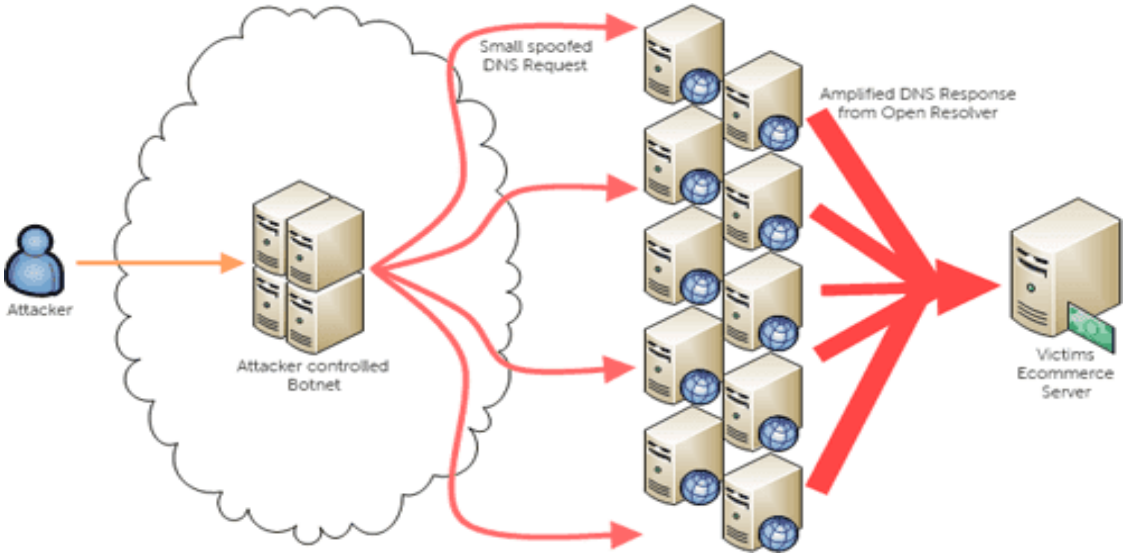
Đây là một dạng tấn công từ chối dịch vụ (DDoS). Kẻ tấn công sử dụng các máy chủ DNS mở (trả lời truy vấn từ mọi địa chỉ IP) để làm tràn băng thông của đối tượng cần tấn công.

Có hai yếu tố cơ bản cho cách thức tấn công này:

– Địa chỉ tấn công được che giấu nhờ ánh xạ sang một bên thứ ba (Reflection)

– Traffic mà người bị hại nhận được sẽ lớn hơn traffic gửi từ attacker (Amplification)

Mô tả chi tiết về cách thức hoạt động.



Hình 2-23: Amplification Attack

Để thực hiện một cuộc tấn công DNS Amplification Attacks kẻ tấn công sử các máy chủ DNS mở (trả lời truy vấn dns từ bất kỳ ip nào) để làm tràn băng thông của mục tiêu tấn công. Để làm được việc này kẻ tấn công sẽ gửi các truy vấn DNS đến các máy chủ DNS mở với địa chỉ ip nguồn của gói tin là địa chỉ ip của mục tiêu cần tấn công. Khi các máy chủ DNS mở gửi thông tin DNS trả lời, toàn bộ sẽ được gửi đến mục tiêu cần tấn công. Để tăng hiệu quả của cuộc tấn công kẻ tấn công thường gửi truy vấn mà kết quả trả về càng nhiều thông tin càng tốt. Các cuộc tấn công DNS Amplification Attacksđược ghi nhận thì DNS request giả địa chỉ ip gửi bởi kẻ tấn công thường là kiểu “ANY” (thông tin trả về sẽ là tất cả thông tin về domain trong truy vấn). Trường hợp này kích thước của gói tin trả về thường lớn hơn rất nhiều so với kích thước của DNS request. Do đó với băng thông vừa phải kẻ tấn công có thể tạo ra một băng thông rất lớn đánh vào mục tiêu. Thêm vào đó gói tin trả về đến từ các địa chỉ hợp lệ do đó việc ngăn chặn cuộc tấn công kiểu này rất khó khăn.

Thực hiện cuộc tấn công.

Dò tìm các máy chủ DNS mở.

Để dò tìm các địa chủ máy chủ DNS mở ta có thể dùng nmap

nmap -sU -p 53 -sV -P0 --script "dns-recursion" 1.1.1.1/24

trong đó 1.1.1.1/24 là dải ips ta muốn scan.

Thực hiện cuộc tấn công.

Để tạo được DNS request với địa chỉ ip là địa chỉ ip mục tiêu ta cần một server hoặc vps có hỗ trợ việc giả ip. Việc tạo DNS request có thể thực hiện đơn giản bằng scapy

```
sr1(IP(src="victim ip),
dst="192.168.5.1")/UDP()/DNS(rd=1,qd=DNSQR(qname="www.slashdot.org")))
```

Bạn cần lập trình một chút để tạo DNS request từ một list các máy chủ DNS, và tạo DNS request kiểu “ANY” nữa :D.

Tăng cường khả năng tấn công.

Bạn cần có một domain sau đó vào tạo nhiều nhất record có thể. record TXT có độ dài lớn, cả CNAME cả A … để tăng băng thông tấn công nên mức cao nhất.

Qua những gì đã trình bày ta thấy cuộc tấn công DNS Amplification Attacks rất khó để có thể ngăn chặn, do đó cần có một chiến lược được hoạch định kỹ để phòng chống loại tấn công này.

2.2.3. Giả mạo máy chủ DNS (DNS Cache):

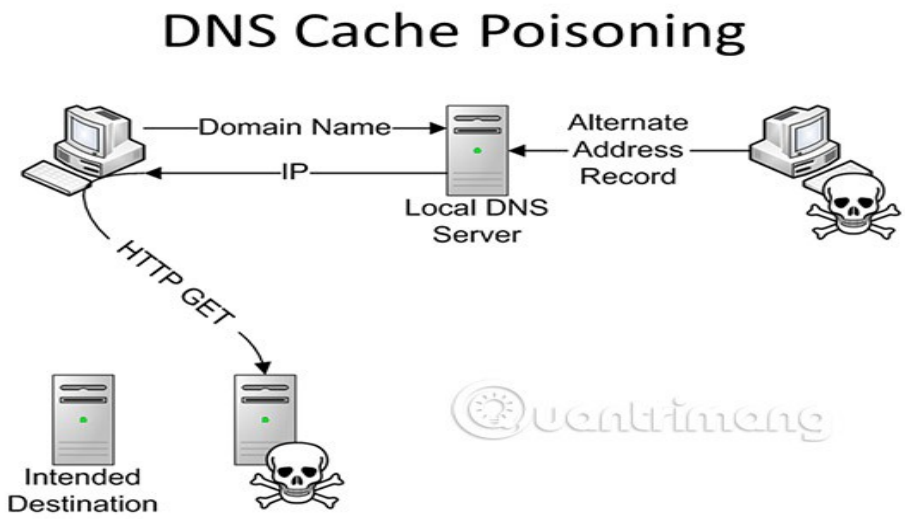
Đây là cách một số phần mềm quảng cáo hay trojan thường hay thực hiện. Đầu tiên, chúng dựng lên các DNS server, giống với chức năng DNS server thông thường. Tuy nhiên, các DNS server này có khả năng điều khiển được để thêm, bớt hay chỉnh sửa các bản ghi DNS nhằm chuyển hướng người dùng tới các địa chỉ IP không chính xác với mục đích: gia tăng quảng cáo, cài mã độc, thay đổi kết quả tìm kiếm…

Để thực hiện hành vi này, các phần mềm độc hại sau khi được cài vào máy tính người dùng, chúng sẽ tìm cách để thay đổi cấu hình DNS của người dùng thành địa chỉ DNS của phần mềm đã thiết lập từ trước. Qua đó, các truy vấn DNS của người dùng thay vì đi qua các DNS server của ISP hoặc do người dùng thiết lập thì lại đi qua các DNS server của attacker.

Một biến thể của hình thức này chính là việc các phần mềm độc hại thay đổi file host (Trên hệ điều hành Windows) để chỉ định địa chỉ IP cho một số website mà attacker mong muốn.

2.2.3.1. Làm nhiễm độc DNS cache:

Mỗi lần người dùng nhập URL trang web vào trình duyệt của mình, trình duyệt sẽ liên hệ với một file cục bộ (DNS Cache) để xem có bất kỳ mục nhập nào giống với địa chỉ IP của trang web hay không. Trình duyệt cần địa chỉ IP của các trang web để nó có thể kết nối với trang web đó. Nó không thể chỉ sử dụng URL để kết nối trực tiếp với trang web. Nó phải được kết nối vào một địa chỉ IP IPv4 hoặc IPv6 thích hợp. Nếu bản ghi ở đó, trình duyệt web sẽ sử dụng nó; nếu không nó sẽ đi đến một máy chủ DNS để có được địa chỉ IP. Điều này được gọi là DNS Lookup.



Hình 2-24: DNS Cache Poisoning

Bộ nhớ DNS cache được tạo trên máy tính hoặc máy chủ DNS ISP của bạn để lượng thời gian dành cho việc truy vấn DNS của một URL giảm xuống. Về cơ bản, DNS cache là các file nhỏ chứa địa chỉ IP của các trang web khác nhau thường được sử dụng trên máy tính hoặc mạng. Trước khi liên hệ với máy chủ DNS, máy tính trên mạng liên hệ với máy chủ cục bộ để xem có bất kỳ mục nhập nào trong bộ nhớ DNS cache hay không. Nếu có, máy tính sẽ sử dụng nó. Nếu không máy chủ sẽ liên lạc với máy chủ DNS và tìm nạp địa chỉ IP đó. Sau đó, nó sẽ cập nhật bộ nhớ DNS cache cục bộ với địa chỉ IP mới nhất cho trang web.

Mỗi mục nhập trong bộ nhớ DNS cache được đặt giới hạn thời gian, tùy thuộc vào hệ điều hành và độ chính xác của DNS resolution. Sau khi hết hạn, máy tính hoặc máy chủ chứa DNS cache sẽ liên hệ với máy chủ DNS và cập nhật mục nhập sao cho thông tin chính xác.

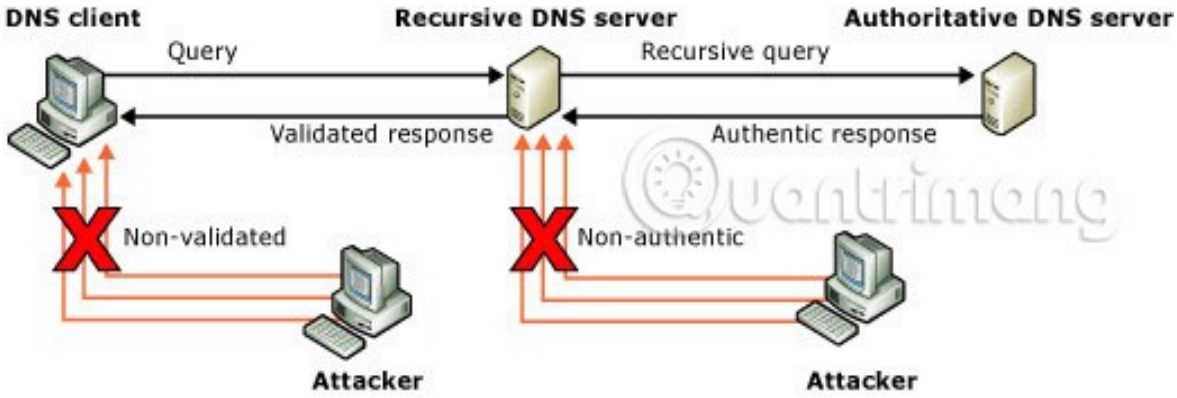
Tuy nhiên, có những người muốn làm nhiễm độc DNS cache cho mục đích xấu.

Làm nhiễm độc bộ nhớ cache có nghĩa là thay đổi giá trị thực của URL. Ví dụ, tội phạm mạng có thể tạo một trang web trông giống như xyz.com và nhập bản ghi DNS của nó vào DNS cache của bạn. Do đó, khi bạn gõ xyz.com vào thanh địa chỉ của trình duyệt, trình duyệt thứ hai sẽ nhận địa chỉ IP của trang web giả mạo và đưa

bạn đến đó, thay vì trang web thực. Điều này được gọi là Pharming. Sử dụng phương pháp này, bọn tội phạm mạng có thể phát hiện các thông tin xác thực đăng nhập của bạn và nhiều thông tin khác như chi tiết thẻ, số an sinh xã hội, số điện thoại v.v... để ăn cắp dữ liệu cá nhân. Việc làm nhiễm độc DNS cache cũng được thực hiện để đưa phần mềm độc hại vào máy tính hoặc mạng của bạn. Khi bạn truy cập trang web giả mạo bằng bộ nhớ DNS cache bị nhiễm độc, bọn tội phạm có thể làm bất cứ điều gì chúng muốn.

Đôi khi, thay vì bộ nhớ cache cục bộ, bọn tội phạm cũng có thể thiết lập máy chủ DNS giả mạo để khi được truy vấn, chúng có thể phát ra địa chỉ IP giả mạo. Đây là cấp độ cao của việc làm nhiễm độc DNS và làm hỏng hầu hết các DNS cache trong một khu vực cụ thể, do đó ảnh hưởng đến nhiều người dùng hơn.

2.2.3.2. Giả mạo DNS Cache:



Hình 2-25: Giả mạo DNS Cache

Giả mạo DNS là một loại tấn công liên quan đến việc mạo danh các phản hồi của máy chủ DNS, nhằm đưa ra thông tin sai lệch. Trong một cuộc tấn công giả mạo, một tin tặc sẽ cố gắng phán đoán một máy khách DNS hoặc máy chủ đã gửi một truy vấn DNS và đang chờ phản hồi DNS. Một cuộc tấn công giả mạo thành công sẽ chèn một phản hồi DNS giả vào bộ nhớ cache của máy chủ DNS. Quá trình này được gọi là làm nhiễm độc bộ nhớ cache. Một máy chủ DNS giả mạo không có cách xác minh rằng dữ liệu DNS là xác thực và sẽ trả lời từ bộ nhớ cache của nó bằng cách sử dụng thông tin giả mạo.

Giả mạo DNS cache có vẻ tương tự như làm nhiễm độc DNS cache, nhưng có một chút khác biệt nhỏ. Giả mạo DNS cache là một tập hợp các phương pháp được

sử dụng để làm nhiễm độc một bộ nhớ DNS cache. Điều này có thể là một mục nhập bắt buộc vào máy chủ của mạng máy tính để sửa đổi và điều khiển bộ nhớ DNS cache. Điều này có thể thiết lập một máy chủ DNS giả để gửi đi phản hồi giả mạo khi truy vấn. Có rất nhiều cách để làm nhiễm độc một bộ nhớ DNS cache, và một trong những cách phổ biến là giả mạo DNS Cache.

2.3: BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG DNS.

Thông thường thì rất khó để người dùng có thể nhận biết được máy tính cá nhân của mình đang bị tấn công thông qua hệ thống DNS vì có khá ít các dấu hiệu khi bị tấn công. Thông thường, chúng ta không hề biết DNS của mình bị tấn công, giả mạo cho tới khi điều đó xảy ra. Những gì chúng ta nhận được là một trang web khác hoàn toàn so với những gì mong đợi. Trong các tấn công với chủ đích lớn, rất có thể người sử dụng sẽ không hề biết rằng mình đã bị lừa nhập các thông tin quan trọng của mình vào một website giả mạo cho tới khi nhận được cuộc gọi từ ngân hàng hỏi tại sao ta lại rút nhiều tiền đến vậy. Mặc dù khó nhưng không phải không có biện pháp nào có thể phòng chống các kiểu tấn công này, đây là một số cách mà chúng ta cần thực hiện:

- Không có nhiều phương pháp có thể ngăn chặn việc làm nhiễm độc DNS cache. Phương pháp tốt nhất là tăng quy mô hệ thống bảo mật của bạn, để không kẻ tấn công nào có thể xâm phạm mạng của bạn và tác động vào bộ nhớ DNS cache cục bộ. Sử dụng tường lửa tốt có thể phát hiện các cuộc tấn công làm nhiễm độc DNS cache. Xoá bộ nhớ DNS cache thường xuyên cũng là một tùy chọn mà bạn có thể cân nhắc.

- Ngoài việc mở rộng quy mô hệ thống bảo mật, quản trị viên nên cập nhật phần cứng và phần mềm của mình để giữ cho hệ thống hiện tại được bảo mật. Hệ điều hành nên được sửa lỗi với các bản cập nhật mới nhất và không được có bất kỳ liên kết gửi đi của bên thứ ba nào. Máy chủ phải là giao diện duy nhất giữa mạng và Internet cũng như phải được bảo vệ bằng tường lửa tốt.

+ Các mối quan hệ tin cậy của các máy chủ trong mạng phải được đẩy lên cao hơn, để chúng không yêu cầu bất kỳ máy chủ nào khác cho DNS resolution. Bằng

cách đó, chỉ các máy chủ có chứng chỉ chính hãng mới có thể giao tiếp với máy chủ mạng trong khi phân giải các máy chủ DNS.

+ Khoảng thời gian cho mỗi mục nhập trong DNS cache phải ngắn để các bản ghi DNS được tìm nạp thường xuyên và cập nhật hơn. Điều này cũng có thể có nghĩa là khoảng thời gian này sẽ dài hơn khi kết nối với các trang web (chỉ đôi khi thôi) nhưng sẽ làm giảm nguy cơ sử dụng bộ nhớ cache bị nhiễm độc.

+ DNS Cache Locking (khóa DNS Cache) nên được cấu hình đến 90% hoặc cao hơn trên hệ thống Windows của bạn. Khóa bộ nhớ cache trong Windows Server cho phép bạn kiểm soát xem thông tin trong DNS cache có bị ghi đè hay không.

+ Hãy sử dụng DNS Socket Pool vì nó cho phép một máy chủ DNS sử dụng ngẫu nhiên cổng nguồn khi phát ra các truy vấn DNS. Điều này cung cấp bảo mật nâng cao, chống lại các cuộc tấn công làm nhiễm độc bộ nhớ cache (theo TechNet).

+ Domain Name System Security Extensions (DNSSEC) - Các phần mở rộng bảo mật hệ thống tên miền - là một tập hợp các phần mở rộng cho Windows Server để tăng cường thêm bảo mật cho giao thức DNS.

+ Đơn giản nhất chúng ta có thể kiểm tra địa chỉ DNS server trên máy tính của mình, kiểm tra nội dung file host (Hệ điều hành windows). Chú ý sự thay đổi bất thường về giao diện, nội dung của các website thông thường.

+ Bảo vệ các máy tính bên trong: Các tấn công giống như trên thường được thực thi từ bên trong mạng của người sử dụng. Nếu các thiết bị mạng của an toàn thì sẽ người sử dụng sẽ giảm được khả năng các host bị thỏa hiệp và được sử dụng để khởi chạy tấn công giả mạo.

+ Xây dựng máy chủ Sinkhole để phát hiện botnet.

+ Đặt mật khẩu mạnh cho các DNS server.

+ Chúng ta cần thiết lập địa chỉ DNS server trỏ về các DNS server tin cậy, thường xuyên kiểm tra các thông số cấu hình DNS, cài đặt các phần mềm antivirus để bảo vệ máy tính và truy cập tốt hơn.

+ Ngăn không cho thực hiện chuyển vùng trái phép bằng cách sử dụng Access control list, chỉ những máy tính nào có địa chỉ IP nằm trong danh sách này được thực hiện quá trình chuyển vùng với DNS Server chính.

+ Sử dụng IDS: Một hệ thống phát hiện xâm nhập, khi được đặt và triển khai đúng, có thể vạch mặt các hình thức giả mạo ARP cache và giả mạo DNS.

Kết luận chương 2: Nội dung chương 2 cho ta thấy được các lỗ hổng, điểm yếu tồn tại trong hệ thống DNS và hiểu rõ các cách thức tấn công thông dụng mà attacker sử dụng để tấn công vào hệ thống DNS, qua đó phân tích, đánh giá được các kiểu tấn công đó và đưa ra được biện pháp phòng chống.

CHƯƠNG 3. CHƯƠNG 3: CÀI ĐẶT VÀ THỬ NGHIỆM MỘT SỐ GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG

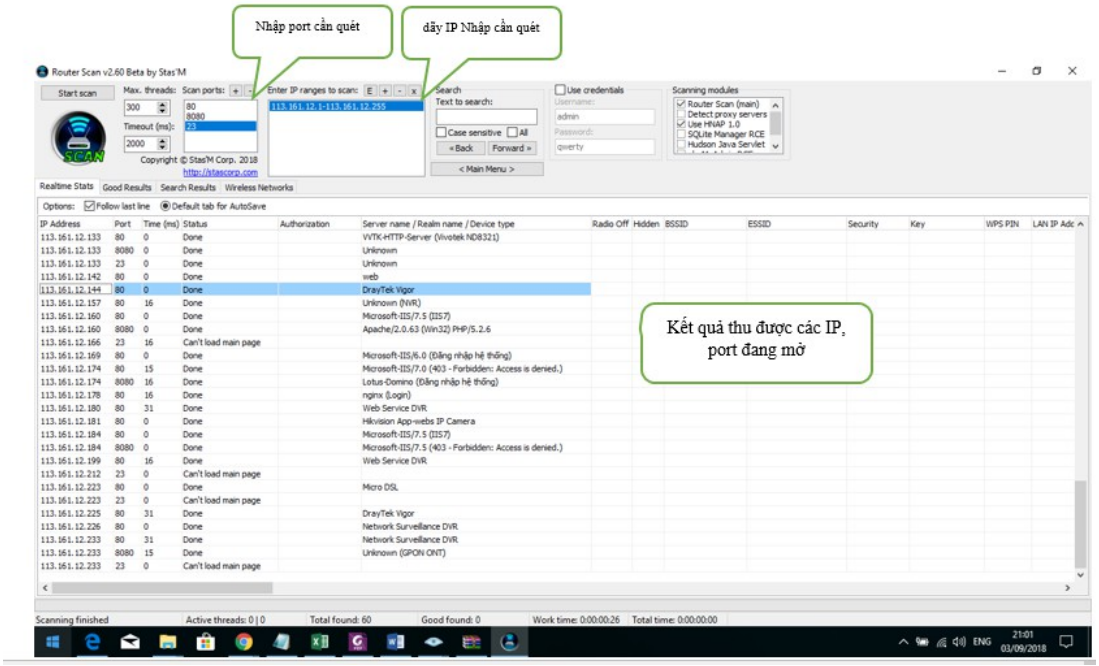
3.1. TẤN CÔNG VÀO THIẾT BỊ IOT CỦA VNPT ĐỔI DNS ĐỂ LÀM GIÁN ĐOẠN TRUY CẬP DỊCH VỤ:

+ Có nhiều cách để tấn công vào thiết bị IoT để thay đổi DNS, ở đây tôi chọn cách tuy cập lỗ hổng qua môi trường internet.

+ Kịch bản quá trình thực hiện:

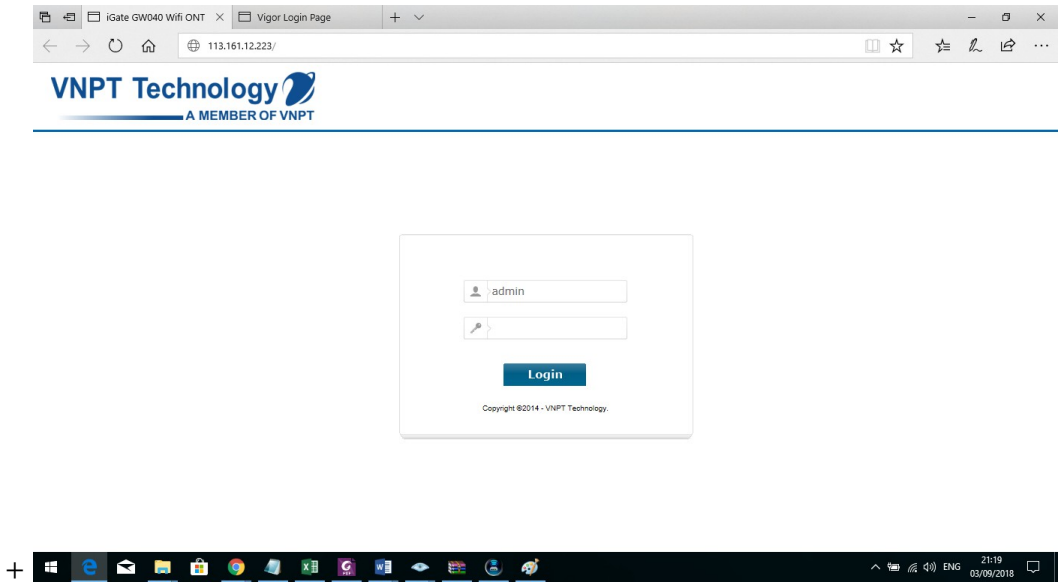
- Chuẩn bị máy tính, cài đặt phần mềm quét tìm kiếm các thiết bị có kết nối Internet trên mạng. Trong trường hợp này mình sử dụng phần mềm RouterScan.exe *(link download, https://www.rekings.com/router-scan/)*, nó sẽ tìm kiếm tất cả các thiết bị có kết nối Internet từ Router, Webcam, Server,…… có thể hiển thị chi tiết các port đang mở.

- Sau khi cài đặt có giao diện như hình và nhập các thông tin, pool Ip wan nhà cung cấp dịch vụ cần quét lỗ hổng:



Hình 3-26: Quét lỗ hổng thiết bị

- Sau khi xác định được đối tượng cần tấn công, mình truy nhập từ xa qua internet theo địa chỉ IP Wan hoặc IP Lan để đăng nhập vào Modem và kết quả thu được:



Hình 3-27: Giao diện đăng nhập thiết bị

Khi nó mở ra một trang web yêu cầu tên người dùng và mật khẩu như hình trên, hãy thử một trong các kết hợp sau đây:

admin / admin

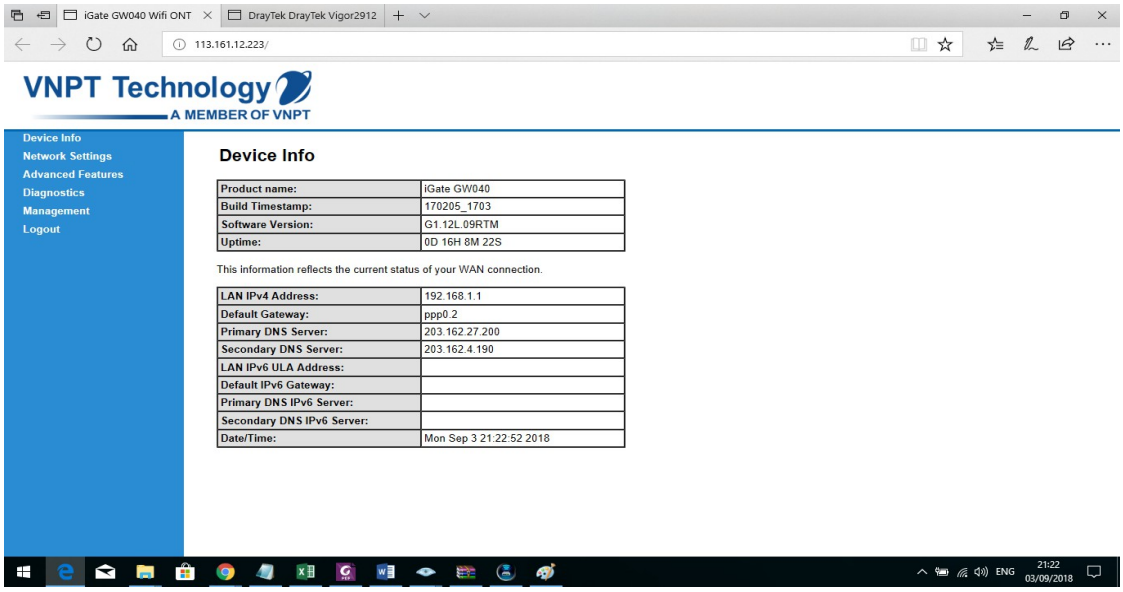
admin / password

admin / pass

admin / root

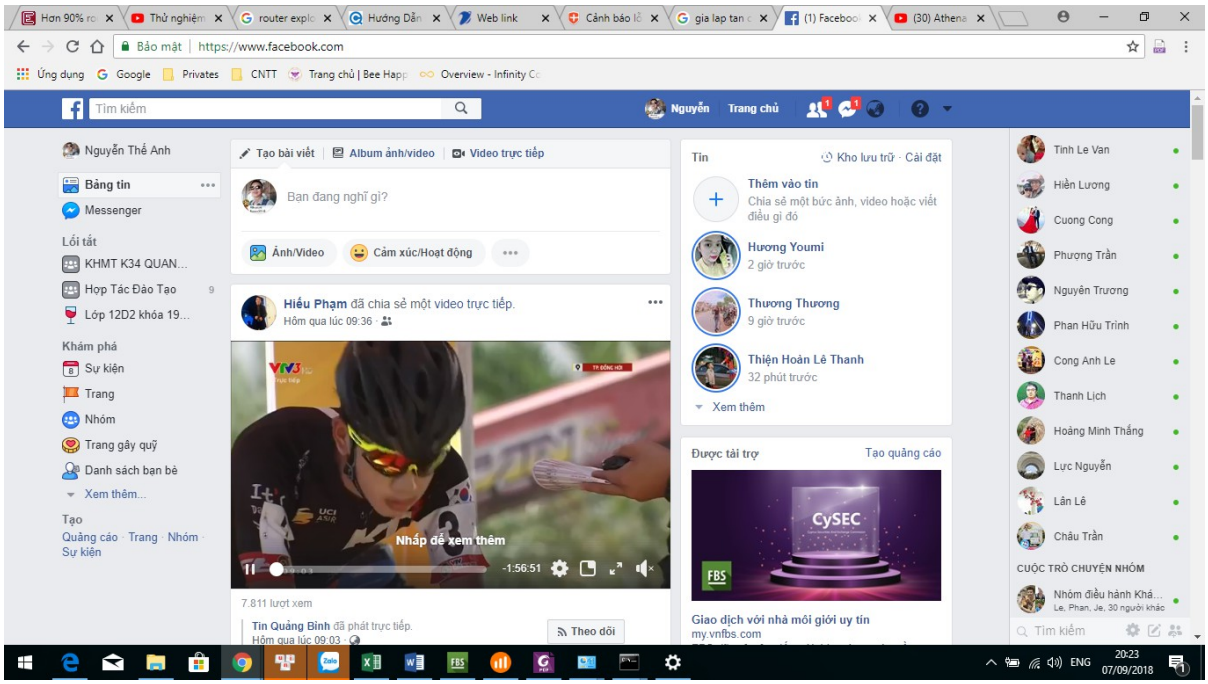
Sau khi đăng nhập vào được modem, nhiệm vụ của mình là thay đổi DNS của nhà cung cấp dịch vụ sang một DNS giả mạo để làm cho dịch vụ của khách hàng bị gián đoạn, hoặc là có các mục đích khác nhằm làm ảnh hưởng dịch vụ của khách hàng, đánh cắp thông tin của khách hàng và làm suy giảm uy tính của nhà cung cấp dịch vụ. Và mình đã thấy kết quả hiện trạng các thông số DNS của nhà cung cấp dịch vụ:

DNS mặc định của nhà cung cấp dịch vụ



Hình 3-28: Xem DNS mặc định

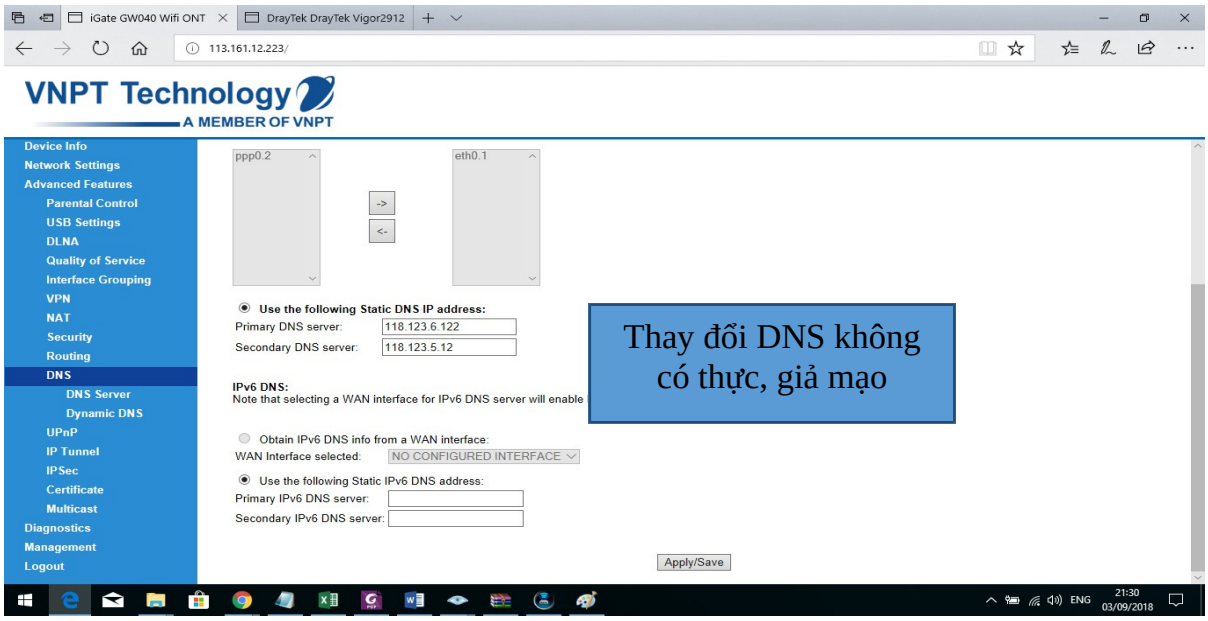
Dịch vụ của khách hàng trước khi tấn công thay đổi DNS modem, Khách hàng vẫn sử dụng được dịch vụ internet bình thường:



Hình 3-29: Truy cập dịch vụ trước khi thay đổi DNS

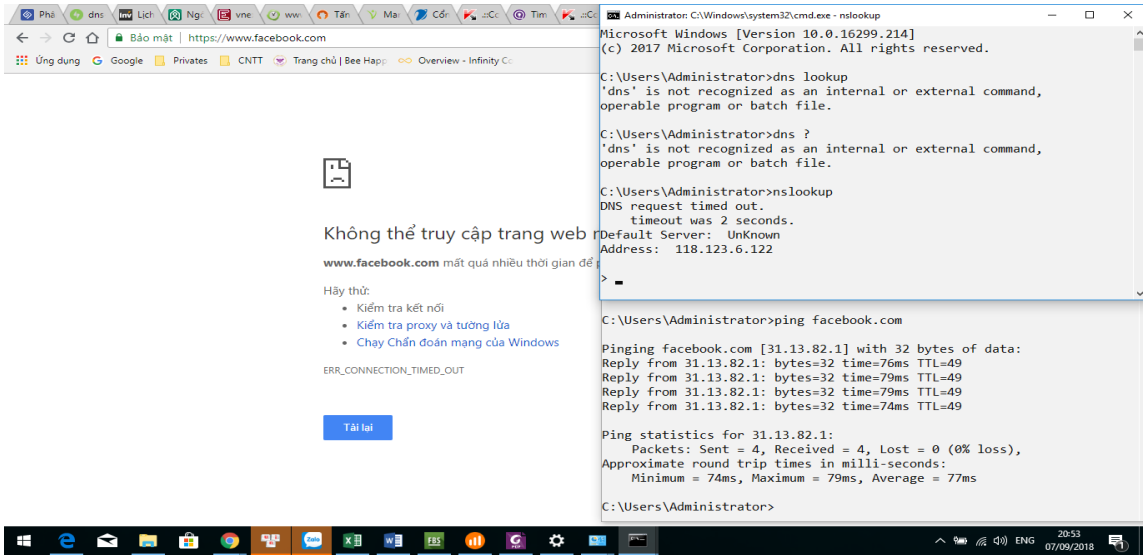
- Tiến hành thực hiện đổi DNS của mặc định của nhà cung cấp dịch vụ sang DNS

Tôi đăng nhập vào modem, tìm đến mục DNS và gõ vào địa chỉ DNS giả mạo để ngăn chặn truy cập dịch vụ của khách hàng:

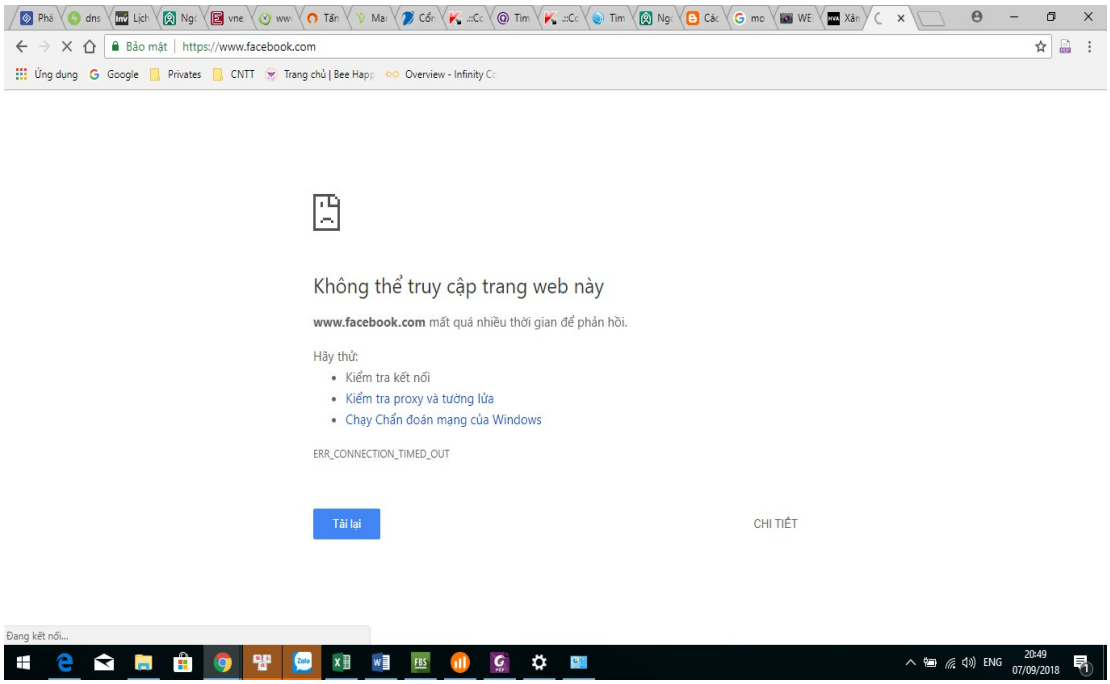


Hình 3-30: Thay đổi DNS giả mạo

- Dịch vụ của khách hàng sau khi tấn công thay đổi DNS modem: không thể truy cập được dịch vụ mặc dù kiểm tra kết nối vật lý vẫn bình thường (vẫn ping thông đến server):



Hình 3-31: Kiểm tra kết nối vật lý

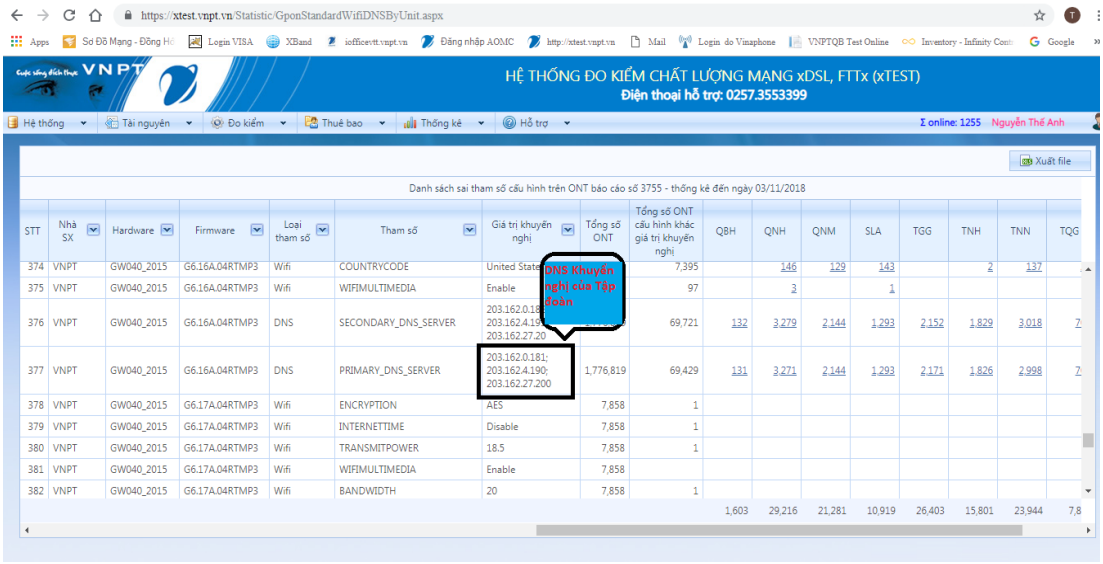


Hình 3-32: Truy cập dịch vụ sau khi thay đổi DNS

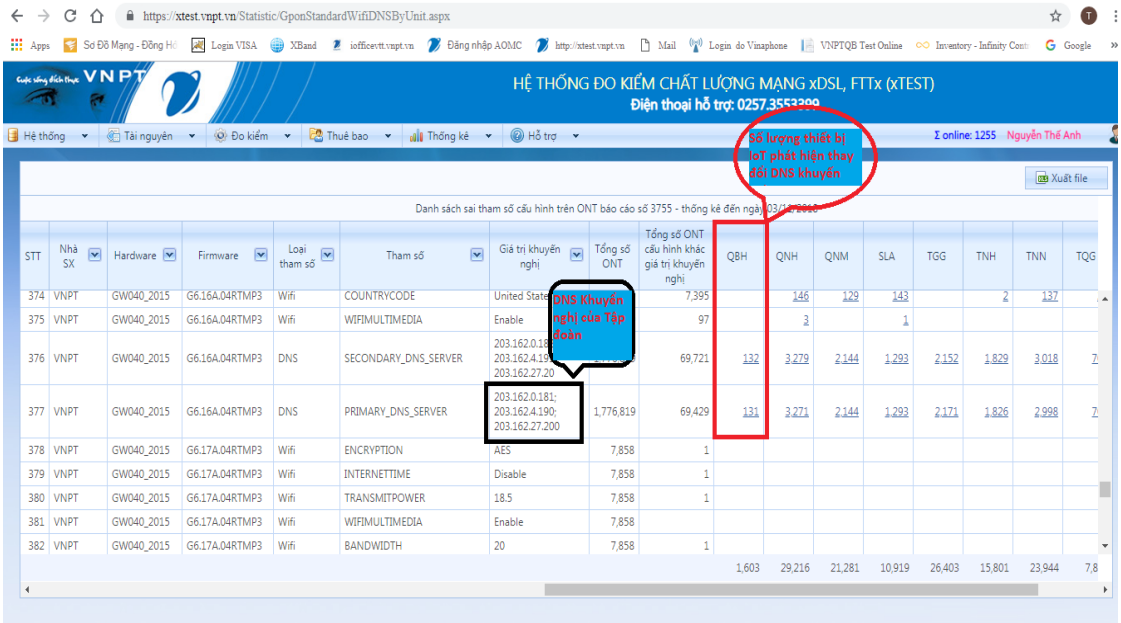
3.2. **PHƯƠNG PHÁP PHÁT HIỆN NHỮNG THAY ĐỔI DNS BẤT THƯỜNG VÀ GIẢI PHÁP XỬ LÝ CHO THIẾT BỊ IOT TỪ XA.**

3.2.1. **Phương pháp phát hiện thay đổi bất thường DNS của thiết bị IoT:**

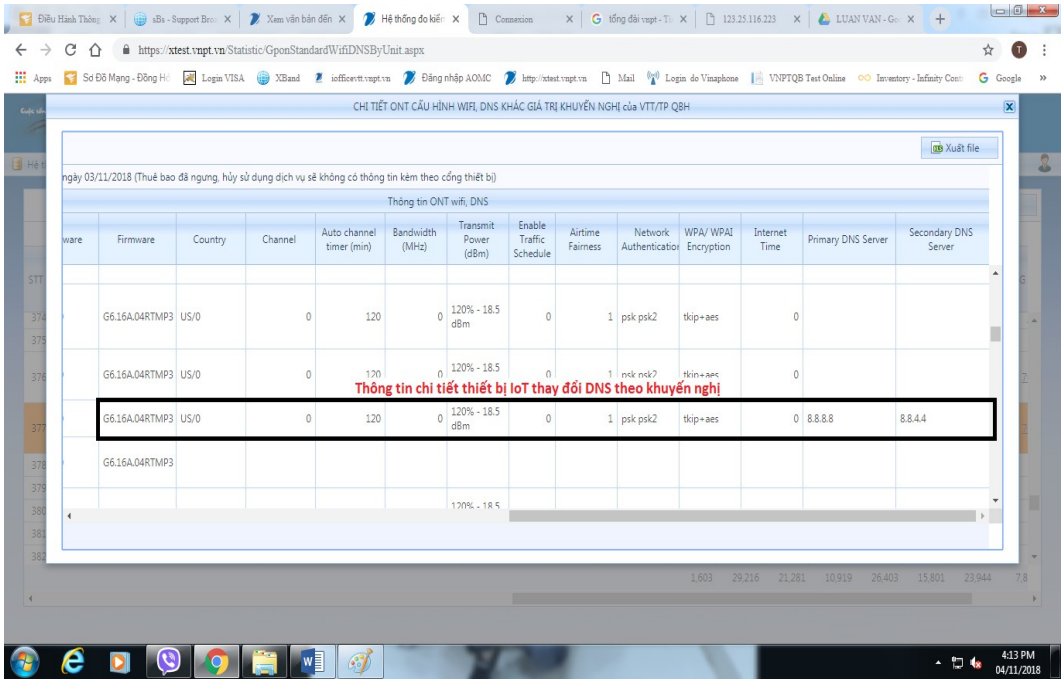
- Để phát hiện những thay đổi bất thường trên hệ thống thiết bị của khách hàng, tôi đã ứng dụng phần mềm xTest (xtest.vnpt.vn) của Tập đoàn để thực hiện quét, lọc và phát hiện những thay đổi DNS bất thường định kỳ:



Hình 3-33: Xem DNS được khuyến nghị trên xTest



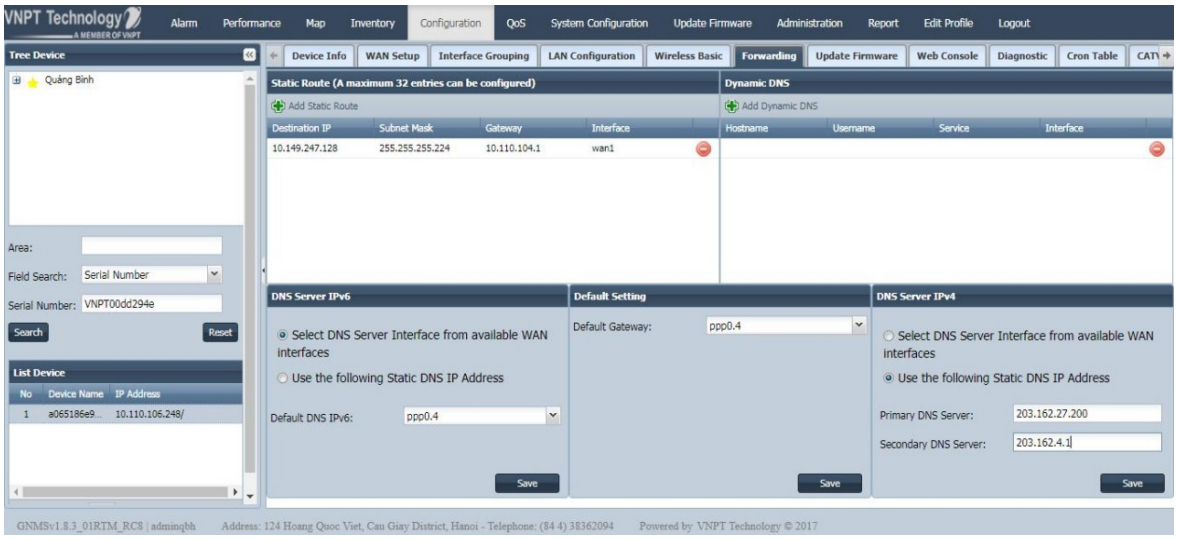
Hình 3-34: Hiển thị tổng hợp thiết bị bị thay đổi DNS



Hình 3-35: Danh sách chi tiết thiết bị bị thay đổi DNS

3.2.2. Giải pháp xử lý DNS cho thiết bị IoT từ xa**:**

- Sử dụng phần mềm GNMS: Ứng dụng được phát triển bởi VNPT-Technology, trợ giúp cho nhân viên kỹ thuật thuận tiện hơn trong việc hỗ trợ xử lý các lỗi phát sinh từ các thiết bị của khách hàng .



Hình 3-36: Thay đổi DNS từ xa trên GNMS

3.3. **ĐỀ XUẤT CÁC BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG THIẾT BỊ IOT TRONG MẠNG VNPT QUẢNG BÌNH.**

- Nâng cấp Fimware cho thiết bị router lên phiên bản mới đã được sữa lỗi (đã thực hiện).

- Đổi mật khẩu đăng nhập mặc định đăng nhập vào modem (đã thực hiện)

- Tắt chức năng truy cập từ xa router qua internet (web, telnet…)

- Thay đổi Cổng quản lý web- Truy cập trình duyệt web thông thường sử dụng cổng dịch vụ HTTP chuẩn là 80. Cổng quản lý web từ xa mặc định của Router là 80. Để bảo mật tốt hơn, bạn có thể thay đổi cổng quản lý từ xa khác bằng cách nhập vào số trong ô được cung cấp. Chọn một số từ 1 đến 65535 nhưng không sử dụng số thuộc về các cổng thông thường.

Kết luận chương 3: Nội dung chương 3 cho ta một cái nhìn trực quan, cụ thể về một cuộc tấn công vào các thiết bị IoT diễn ra như thế nào. Từ đó hiểu rõ hơn và đưa ra được các biện pháp phòng chống đặc biệt là các cuộc tấn công thay đổi, thay đổi, giả mạo DNS, và các biện pháp phòng chống đó trong thực tế.

KẾT LUẬN VÀ KIẾN NGHỊ

Sau thời gian làm luận văn sinh viên đã hoàn thiện được và luận văn chỉ ra được các mối nguy hiểm khi bị tấn công và đề xuất giải pháp ngăn chặn cũng như hạn chế tác hại của hình thức tấn công trên mạng internet. Từ đó xây dựng và thử nghiệm một số giải pháp đối với đối tượng là các doanh nghiệp vừa và nhỏ. Đánh giá hiệu quả của các biện pháp đã xây dựng và làm tiền đề để phát triển các nghiên cứu sau này. Sinh viên đã tìm hiểu tương đối thành công về DNS và xây dựng được thành công phương pháp phòng thủ DNS. Với những gì đã tìm hiểu được, sinh viên vẫn cảm thấy có nhiều điều cần phải làm để hoàn thiện hơn luận văn cũng như cách làm thực tế trong công việc. Bản thân sinh viên cần phải có sự hướng dẫn nhiều hơn từ thầy cô và bạn bè.

- Kết quả đạt được.

- Tìm hiểu khái niệm về DNS.
- Tìm hiểu các loại và các kiểu tấn công DNS.
- Tìm hiểu được một số công cụ tấn công DNS và một vài ví dụ thực tế về tác hại các cuộc tấn công DNS nhắm đến mục tiêu là các doanh nghiệp vừa và nhỏ.
- Triển khai thành công giải pháp phòng chống thay đổi, giả mạo DNS thực tế hiện nay trên hệ thống mạng của nhà cung cấp dịch vụ và đưa ra một số cách phống chống.

- Hướng phát triển của luận văn.

Do thời gian có hạn cũng như hạn chế về cơ sở vật chất cho nên việc tìm hiểu cũng như xây dựng hệ thống phòng thủ DNS vẫn còn nhiều hạn chế và thiếu sót. Sinh viên hi vọng rằng trong tương lai gần có thể xây dựng, thử nghiệm nhiều giải pháp phòng thủ còn lại đã nêu trong bài và đánh giá cũng như so sánh giữa các giải pháp hoặc tích hợp thêm một vài giải pháp để có được giải pháp phòng thủ tối ưu hơn trước các cuộc tấn công lớn vào hệ thống DNS.

Vấn đề an toàn thông tin và bảo mật ngày nay đang được các cơ quan, nhà bảo mật và đặc biệt là các doanh nghiệp quan tâm hàng đầu. An toàn dữ liệu, thông tin người dùng, và tài chính của công ty, mọi vấn đề đều cần được quan tâm. Đối với doanh nghiệp, thì quan trọng nhất là thông tin cá nhân, tài khoản của người dùng, ví dụ như ngân hàng chẳng hạn, các thông tin này phải được bảo mật tuyệt đối, vì thế vấn đề bảo mật đang là một thách thức lớn cho các nhà doanh nghiệp.

Thông qua luận văn, chúng ta đã thấy được một cách tổng quát về hệ thống tên miền DNS, kỹ thuật tấn công dịch vụ DNS, chúng ta có thể hiểu được phần nào nguyên lý, cơ chế tấn công của hacker khi muốn ăn cắp thông tin tài khoản của người dùng. Với các kỹ thuật như tấn công đầu độc DNS, ARP hoặc DHCP sẽ giúp cho kẻ tấn công có thể dễ dàng lấy được thông tin của người dùng khi họ không để ý, hoặc không cẩn thận khi trao đổi dữ liệu trong môi trường mạng công cộng. Hơn thế nữa, nếu thông tin cá nhân của người dùng hoặc công ty bị hacker ăn cắp thì nguy cơ mất dữ liệu hoặc dữ liệu bị truyền ra ngoài sẽ gây một thất thoát lớn cho công ty, và sẽ làm tổn hại nguồn tài chính của công ty hoặc doanh nghiệp.

Để khắc phục và ngăn chặn kịp thời các trường hợp bị tấn công hoặc ăn cắp dữ liệu bởi hacker, thì các doanh nghiệp, tổ chức, cá nhân cần quan tâm và chú trọng hơn nữa về vấn đề bảo mật. Sử dụng SNSSEC, DNS Anycast, dùng Firewall cứng hoặc mềm để ngăn chặn, giảm bớt sự tấn công từ bên ngoài, hoặc cấu hình bảo mật port cho switch để ngăn chặn sniffer, cấu hình các dịch vụ phát hiện và chống xâm nhập trên Server để kịp thời phát hiện các sự cố khi bị hacker tấn công. Ngoài ra, các doanh nghiệp cần backup dữ liệu của khách hàng để đề phòng trường hợp bị mất dữ liệu.

TÀI LIỆU THAM KHẢO

[1]: Thuyết minh dự thảo tiêu chuẩn quốc gia – Các yêu cầu và hướng dẫn bảo mật DNS (DNSSEC) – 2016.

[2] https://voer.edu.vn/m/dich-vu-phan-giai-ten-mien-dns-server/52c04351.Truy cập ngày 26/8/2018.

[3] https://www.slideshare.net/SnowBlack93/h-thng-dns.Truy cập ngày 22/8/2018

[4] http://itforvn.com/tu-hoc-mcse-2016-lab-3-cau-hinh-dns-server-tren-windows-server-2016.html/. Truy cập ngày 22/4/2018.

[5] http://text.123doc.org/document/2563875-tim-hieu-va-mo-phong-tan-cong-dich-vu-dns.htm. Truy cập ngày 26/8/2018.

[6] https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/. Truy cập ngày 28/7/2018.

[7] Giáo trình Hệ thống mạng Linux, Mạng máy tính. Nguyễn Tấn Khôi, khoa CNTT, Đại học Bách khoa Đà Nẵng.

[8] https://whitehat.vn/threads/dns-tu-duy-hoat-dong-dns-co-che-hoat-dong-dns-mot-so-thong-tin-chi-tiet-hon-ve-dns.4702/ Truy cập ngày 2/8/2018

[9] https://www.engisv.info/?p=162 Truy cập ngày 22/8/2018