HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÁO CÁO
AN TOÀN HỆ MẠNG

NHÓM 4
GIAO THỨC DNS

B20DCAT206 - Nguyễn Việt Đông

B20DCAT042 - Lương Ngọc Đức

B20DCAT047 - Phạm Minh Đức

B20DCAT056 - Dương Ngô Hiếu

B20DCAT074 - Hoàng Thạch Hùng

I. Giới thiệu về kiến trúc DNS

1. Khái niệm

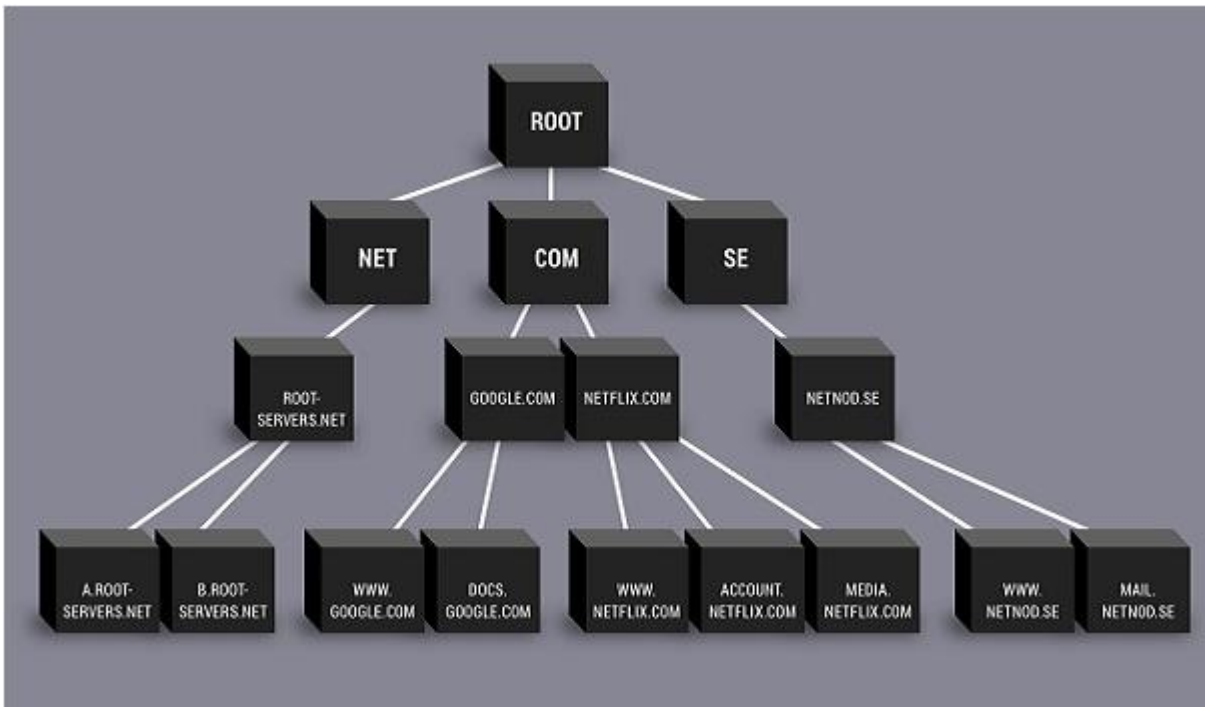
DNS là viết tắt của *"Domain Name System"* (Hệ thống Tên Miền), là một giao thức quan trọng trong hạ tầng Internet. Nó cung cấp một cách để ánh xạ các tên miền thành địa chỉ IP mà máy tính có thể hiểu.

2. Kiến trúc DNS

DNS bao gồm nhiều thành phần quan trọng, bao gồm các thành phần chính sau:

- **DNS Client (Resolver):** Đây là phần mềm hoặc phần của hệ điều hành trên máy tính người dùng cuối, có trách nhiệm gửi yêu cầu DNS đến các máy chủ DNS để tìm kiếm địa chỉ IP cho một tên miền cụ thể.
- **DNS Recursor:** Đây là máy chủ phản hồi truy vấn DNS và yêu cầu máy chủ DNS khác cung cấp địa chỉ hoặc đã có địa chỉ IP cho trang Web được lưu.
- **Root Name Server:** Là máy chủ định danh cho vùng gốc (Root Zone). Nó phản hồi các yêu cầu trực tiếp và có thể trả về danh sách các Authoritative Name Server cho tên miền cấp cao nhất tương ứng.
- **TLD Name Server:** Đây là một trong những máy chủ DNS cấp cao trên Internet. Ví dụ, khi bạn tìm kiếm www.google.com, máy chủ TLD cho '.com' sẽ phản hồi đầu tiên, sau đó DNS sẽ tìm kiếm 'Google'.

- **Authoritative DNS Server:** Là điểm dừng cuối cùng cho truy vấn DNS và có bản ghi DNS cho các truy vấn, yêu cầu.
- **Caching DNS Servers:** Là các máy chủ DNS ở mức cơ sở hoặc ở cấp độ của nhà cung cấp dịch vụ Internet (ISP) hoặc tổ chức. Chúng lưu trữ thông tin tên miền đã được truy cập gần đây trong bộ nhớ đệm để giảm thời gian tìm kiếm tên miền.
- **Zone Files:** Là các tệp dữ liệu trên máy chủ DNS Authority chứa thông tin về các bản ghi DNS của tên miền. Các bản ghi này bao gồm thông tin như địa chỉ IP, mail server,v.v.
- **Root Hints File:** Là một tệp dữ liệu trên các DNS Resolver, chứa thông tin về địa chỉ IP của các máy chủ DNS gốc.



3. *Các loại DNS Record.*

DNS sử dụng các loại bản ghi (record types) để ánh xạ tên miền với các giá trị cụ thể như địa chỉ IP, mail server, v.v. Dưới đây là một số loại bản ghi DNS phổ biến:

- **A Record (Address Record) (A):** Loại bản ghi này ánh xạ một tên miền (domain name) với một địa chỉ IPv4.
- **AAAA Record (IPv6 Address Record) (AAAA):** Tương tự như A Record, nhưng ánh xạ tên miền với một địa chỉ IPv6.
- **CNAME Record (Canonical Name):** Chỉ định rằng tên miền (alias) này là bản ghi của một tên miền khác (canonical name). Đây thường được sử dụng để tạo ra các bí danh cho các tên miền chính.
- **MX Record (Mail Exchange) (MX):** Xác định Host Name cho một Mail Server.

- **NS Record (Name Server) (NS):** Bản ghi này có thể chỉ định Name Server cho từng tên miền phụ và bên cạnh đó có thể tạo tên Name Server, TTL hay host mới.
- **Reverse-lookup Pointer Record (PTR):** Cho phép người dùng tra cứu ngược lại nơi họ cung cấp địa chỉ IP và truy xuất Hostname.
- **Start Of Authority (SOA):** Chứa dữ liệu trong DNS Zone cung cấp thông tin quản trị về Zone đó và các bản ghi DNS khác.
- **Text Record (TXT):** Chứa thông tin văn bản có thể đọc được,các thông tin này có thể có giá trị đối với những người khác đang truy cập vào Server.
- **Service Location Record (SRV):** Cho phép người dùng tìm một dịch vụ cụ thể.
- **Certificate Record (CERT):** Hồ sơ về chứng chỉ và danh sách các chứng chỉ đã bị thu hồi (Certificate Revocation List – CRLs) có liên quan.

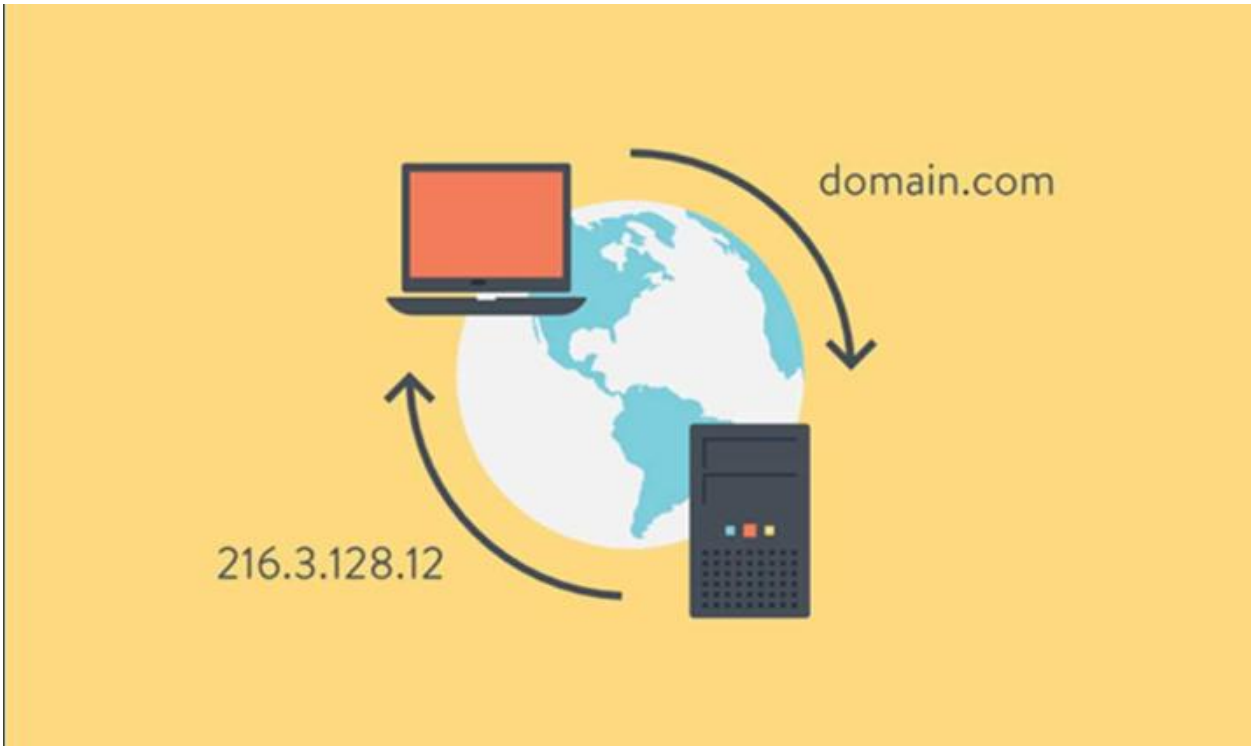
➢ Mỗi loại bản ghi DNS đóng vai trò quan trọng trong việc quản lý và cung cấp các dịch vụ trên Internet. Các bản ghi này cung cấp thông tin cần thiết để tạo ra một kết nối hợp lệ giữa các tên miền và địa chỉ IP hoặc dịch vụ cụ thể.

II. Cơ chế hoạt động của DNS.

DNS hoạt động theo cơ chế sau:

- Bước 1: Khi bạn truy cập một máy tính trên Internet, một yêu cầu DNS sẽ được bắt đầu. Ví dụ bạn nhập www.Google.com vào thanh địa chỉ trình duyệt của mình.
- Bước 2: Điểm dừng đầu tiên cho yêu cầu DNS là bộ nhớ đệm DNS cục bộ (Local DNS Cache). Khi bạn truy cập các máy tính khác nhau, các địa chỉ IP đó được lưu trữ trong kho lưu trữ cục bộ. Nếu bạn đã truy cập www.Google.com trước đây, trong bộ nhớ cache của bạn sẽ có địa chỉ IP này.
- Bước 3: Nếu bạn không có địa chỉ IP trong Local DNS Cache, DNS sẽ kiểm tra bằng Recursive DNS Server.
- Bước 4: Recursive DNS Server có bộ nhớ Cache riêng và nếu có địa chỉ IP, nó sẽ trả lại cho bạn. Nếu không, nó sẽ hỏi một máy chủ DNS khác.
- Bước 5: Điểm dừng tiếp theo là TLD Name Servers. Các máy chủ này có thể không có địa chỉ IP mà bạn cần, nhưng nó có thể gửi yêu cầu DNS theo đúng hướng.
- Bước 6: TLD Name Servers có vị trí của Authoritative Name Server cho trang Web được yêu cầu.
- Bước 7: Dịch vụ DNS cục bộ của bạn lấy địa chỉ IP và kết nối với URL bạn tìm kiếm để tải xuống tất cả nội dung. Sau đó, DNS ghi lại địa chỉ IP trong Local Cache với Time-To-Live (TTL). TTL là khoảng thời gian bản ghi DNS cục bộ hợp lệ, sau thời gian đó, DNS sẽ thực hiện lại quy trình khi bạn yêu cầu URL đã tìm kiếm vào lần tiếp theo.

➢ Quá trình này giúp người dùng truy cập các tài nguyên trên Internet bằng cách sử dụng các tên miền dễ nhớ thay vì phải nhớ các địa chỉ IP phức tạp.



III. Ứng dụng của DNS

DNS có nhiều ứng dụng quan trọng trong hệ thống Internet:

- Truy cập Website: DNS cho phép bạn sử dụng tên miền dễ nhớ thay vì phải ghi nhớ các địa chỉ IP dài và phức tạp.
- Gửi và nhận email: DNS cũng quan trọng trong việc gửi và nhận email, vì nó giúp xác định địa chỉ máy chủ email của người nhận.
- Dịch vụ mạng khác: DNS cũng được sử dụng trong nhiều ứng dụng mạng khác như trò chuyện trực tuyến, truy cập từ xa, và nhiều dịch vụ khác.

IV. Các lỗ hổng bảo mật trong DNS

DNS cũng có một số lỗ hổng bảo mật tiềm ẩn:

- **Cache Poisoning:** Đây là một trong những lỗ hổng bảo mật phổ biến của DNS. Kẻ tấn công cố gắng thêm thông tin giả mạo vào bộ nhớ đệm DNS của máy chủ cục bộ bằng cách gửi các phản hồi DNS giả mạo. Khi thông tin giả mạo được lưu trữ trong bộ nhớ đệm, người dùng có thể bị định hướng đến địa chỉ IP sai.

- **DNS Spoofing**: Còn được gọi là DNS cache poisoning, kỹ thuật này liên quan đến việc đưa thông tin DNS giả mạo vào bộ nhớ đệm DNS, từ đó dẫn dụ người dùng truy cập vào trang web giả mạo thay vì trang web thật sự.
- **Amplification Attacks:** Tấn công DDoS sử dụng các server DNS mở để phản hồi một lượng lớn dữ liệu đến một địa chỉ IP giả mạo.
- **Zone Transfer Attacks:** Khi tấn công viên yêu cầu một bản sao của dữ liệu tên miền từ một DNS Server.
- **Lỗ hổng DNSSEC (DNS Security Extensions):** Mặc dù DNSSEC được thiết kế để cải thiện bảo mật DNS bằng việc ký số hóa các bản ghi DNS, nhưng nó cũng có thể trở thành mục tiêu của tấn công nếu triển khai không đúng cách hoặc không được cập nhật.
- **Kỹ thuật Fast Flux:** Kỹ thuật này liên quan đến việc thay đổi liên tục địa chỉ IP của máy chủ độc hại để tránh bị phát hiện.

V. Các dạng tấn công DNS phổ biến:

DNS Spoofing/Cache Poisoning

Đầu độc bộ nhớ Cache DNS là một kỹ thuật tấn công mà kẻ tấn công cố gắng chèn thông tin DNS giả mạo vào bộ nhớ cache DNS của máy chủ DNS hoặc máy khách. Khi người dùng tìm kiếm một tên miền, máy chủ DNS sẽ truy vấn bộ nhớ cache để tìm kiếm địa chỉ IP tương ứng. Nếu bộ nhớ cache đã bị đầu độc, nó sẽ trả về địa chỉ IP sai, dẫn đến sự chuyển hướng người dùng đến các trang web độc hại hoặc giả mạo.

DNS Amplification

Tấn công này sử dụng các máy chủ DNS để tạo ra một lưu lượng truy cập lớn và gửi nó đến một mục tiêu, làm quá tải hệ thống và gây tắc nghẽn.

DNS Tunneling

Đây là một kỹ thuật tấn công nơi kẻ tấn công sử dụng giao thức DNS để truyền dữ liệu giữa hai máy tính mà không gây sự nhận ra của hệ thống bảo mật.

Giả mạo master trong việc đồng bộ dữ liệu giữa các máy chủ DNS.

Kỹ thuật này liên quan đến tấn công vào quá trình đồng bộ dữ liệu giữa các máy chủ DNS, trong đó kẻ tấn công giả mạo vai trò của máy chủ DNS chính (master). Khi các máy chủ DNS phụ cố gắng đồng bộ dữ liệu từ máy chủ DNS chính, kẻ tấn công sẽ gửi thông tin giả mạo, làm cho các máy chủ phụ nhận dữ liệu sai hoặc độc hại. Điều này có thể dẫn đến việc phân giải DNS sai hoặc truy cập đến các trang web độc hại.

Spoofing master, spoofing update, …

Spoofing master và spoofing update là các kỹ thuật giả mạo trong quá trình gửi và nhận các thông điệp đồng bộ dữ liệu giữa các máy chủ DNS. Kẻ tấn công sẽ giả mạo địa chỉ IP hoặc thông tin chứng thực của máy chủ DNS chính (master), hoặc giả mạo các thông điệp cập nhật DNS để lừa các máy chủ DNS phụ nhận và áp dụng các thay đổi độc hại trong hệ thống DNS.

Chuyển hướng phân giải DNS người dùng sang DNS giả mạo: Man in middle attack.
Trong tấn công này, kẻ tấn công tiếp cận trung gian giữa người dùng và máy chủ DNS chính. Khi người dùng gửi yêu cầu DNS, kẻ tấn công can thiệp vào quá trình truyền thông và chuyển hướng yêu cầu DNS sang một máy chủ DNS giả mạo. Máy chủ DNS giả mạo sau đó sẽ trả về địa chỉ IP sai hoặc trang web độc hại, gian lận người dùng và đánh cắp thông tin nhạy cảm.

Giả mạo hoặc thay đổi các bản ghi trong DNS.

Kỹ thuật này nhằm mục đích thay đổi hoặc giả mạo các bản ghi DNS, chẳng hạn như bản ghi A (địa chỉ IP), bản ghi MX (máy chủ thư), hoặc bản ghi NS (máy chủ tên miền). Kẻ tấn công có thể thực hiện việc này bằng cách xâm nhập vào hệ thống DNS và thay đổi trực tiếp các bản ghi, hoặc sử dụng các kỹ thuật tấn công khác như DNS Cache Poisoning để lừa các máy chủ DNS cập nhật các bản ghi sai hoặc độc hại.

VI. Giải pháp bảo mật DNS

Công nghệ bảo mật DNSSEC

Trước nguy cơ dữ liệu DNS bị giả mạo và bị làm sai lệch trong các tương tác giữa máy chủ DNS với các máy trạm (resolver) hoặc máy chủ chuyển tiếp (forwarder), công nghệ bảo mật **DNSSEC** đã được nghiên cứu, triển khai áp dụng để hỗ trợ cho DNS bảo vệ chống lại các nguy cơ giả mạo làm sai lệch nguồn dữ liệu. DNSSEC là công nghệ an toàn mở rộng của DNS, về bản chất DNSSEC cung cấp các cơ chế có khả năng chứng thực và đảm bảo toàn vẹn dữ liệu cho hệ thống DNS. Trong đó DNSSEC sẽ cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau và xác thực cho từng zone dữ liệu để đảm bảo toàn vẹn dữ liệu

DNSSEC (Domain Name System Security Extensions) là tiêu chuẩn an toàn mở rộng cho hệ thống DNS để đảm bảo việc xác thực và toàn vẹn của dữ liệu trong thông tin trả lời truy vấn tên miền của hệ thống DNS. Sử dụng DNSSEC giúp cho việc truy cập các dịch vụ trên Internet được đảm bảo chính xác, tránh giả mạo vì chúng có các tính năng:

- Chứng thực dữ liệu trong quá trình gửi đi. (Sender authentication)
- Toàn vẹn dữ liệu trong quá trình truyền. (Data Integrity)
- Xác thực từ chối tồn tại. (Authenticated denial of existence)

Ngoài việc sử dụng công nghệ DNSSEC thì bạn còn có thể bảo vệ DNS của mình bằng các giải pháp sau:

- ***Sử dụng DNS Forwarder DNS Forwarder***

DNS Forwarder là một máy chủ DNS được cấu hình để chuyển tiếp các yêu cầu DNS từ máy khách đến các máy chủ DNS khác. Bằng cách sử dụng DNS Forwarder, tất cả các yêu cầu DNS sẽ được gửi đến một máy chủ DNS tin cậy, giúp giảm lượng truy cập trực tiếp vào các máy chủ DNS công khai và giảm khả năng tấn công trực tiếp lên hệ thống DNS.

- ***Sử dụng máy chủ DNS lưu trữ***

Sử dụng máy chủ DNS lưu trữ có nghĩa là cài đặt và cấu hình máy chủ DNS trực tiếp trên hệ thống của bạn. Điều này giúp kiểm soát toàn diện hơn về cấu hình và bảo mật của máy chủ DNS, giảm khả năng bị tấn công từ bên ngoài.

- ***Sử dụng DNS Advertiser DNS Advertiser (Trình quảng cáo)***

DNS Advertiser là một công cụ giúp ẩn danh các máy chủ DNS thực sự bằng cách thêm một lớp trung gian giữa các máy chủ DNS và người dùng cuối. Điều này làm cho máy chủ DNS trở nên khó nhận ra và giảm khả năng bị tấn công trực tiếp.

- ***Sử dụng DNS Resolver DNS Resolver (trình xử lý) là một máy chủ DNS***

DNS Resolver là một máy chủ DNS chịu trách nhiệm tìm kiếm và cung cấp thông tin DNS cho các yêu cầu từ máy khách. Bằng cách sử dụng DNS Resolver, bạn có thể kiểm soát và giám sát việc xử lý yêu cầu DNS, giúp phát hiện và ngăn chặn các cuộc tấn công vào giao thức DNS.

- ***Bảo vệ bộ nhớ đệm DNS***

Lỗ hổng bảo mật phổ biến trong giao thức DNS là tấn công DNS Cache Poisoning, trong đó kẻ tấn công thay đổi dữ liệu DNS trong bộ nhớ đệm của máy chủ DNS. Để bảo vệ bộ nhớ đệm DNS, cần thực hiện các biện pháp như cập nhật phần mềm, giới hạn quyền truy cập vào bộ nhớ đệm, và sử dụng DNSSEC để đảm bảo tính toàn vẹn của dữ liệu DNS.

- ***Bảo mật kết nối bằng DDNS***

Dynamic DNS (DDNS) là một phương pháp cho phép cập nhật địa chỉ IP của máy chủ DNS một cách tự động khi địa chỉ IP thay đổi. Bằng cách sử dụng DDNS, có thể tạo kết nối an toàn giữa máy chủ DNS và các máy khách bằng cách sử dụng các phương thức bảo mật như SSL/TLS.

- ***Ngừng chạy Zone Transfer Zone Transfer (vùng chuyển đổi)***

Zone Transfer là quá trình sao chép dữ liệu DNS từ một máy chủ DNS chủ quản sang một máy chủ DNS phụ. Tuy nhiên, nếu không được cấu hình chính xác, Zone Transfer có thể trở thành điểm yếu của hệ thống DNS và tiềm ẩn lỗ hổng bảo mmật. Ngừng chạy Zone Transfer trừ khi cần thiết, và chỉ cho phép các máy chủ DNS tin cậy được thực hiện quá trình này.

- ***Sử dụng Firewall kiểm soát truy cập DNS***

Thiết lập và cấu hình tường lửa (Firewall) để kiểm soát truy cập vào máy chủ DNS. Tường lửa có thể giới hạn quyền truy cập từ các địa chỉ IP không tin cậy và chặn các yêu cầu DNS độc hại hoặc không hợp lệ.

- ***Cài đặt kiểm soát truy cập vào Registry của DNS***

DNS Registry chứa các thông tin cấu hình quan trọng của máy chủ DNS. Để tăng cường an toàn, cần cài đặt kiểm soát truy cập vào Registry, chỉ cho phép các người dùng có quyền truy cập cần thiết để thực hiện các thay đổi cấu hình.

- ***Cài đặt kiểm soát truy cập vào file hệ thống DNS***

File hệ thống DNS (như file hosts) chứa các thông tin liên quan đến ánh xạ tên miền và địa chỉ IP. Để đảm bảo an toàn, cần cài đặt kiểm soát truy cập vào file hệ thống DNS, chỉ cho phép các người dùng có quyền truy cập cần thiết để thực hiện các thay đổi.

- ***Anycast routing***

Đây là công cụ hữu ích giúp chống lại các cuộc tấn công DDoS, nó hoạt động hiệu quả dựa trên cơ sở cho phép nhiều server chia sẻ 1 địa chỉ IP. Nhờ vậy mà dù DNS bị tấn công thì các server còn lại vẫn không bị ảnh hưởng, hạn chế tổn thất và giảm thiểu hậu quả gây ra.

VII. Demo

Tấn công: DNS Spoofing Attack

1. ***Địa chỉ IP***

- IP máy kali: 192.168.100.3

```
┌──(root㉿pmduc047)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.3  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::20c:29ff:fefb:6e82  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:fb:6e:82  txqueuelen 1000  (Ethernet)
        RX packets 56  bytes 14247 (13.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3423 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- IP máy victim: 192.168.100.151

```
C:\Users\pmduc047win7>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::e81b:c357:f1f0:5137%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.151
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.2
```

2. ***Cấu hình file etter.dns***

- Tạo ra các record (record google và facebook đều trỏ đến web giả mạo)
- Dùng lệnh mousepad /etc/ettercap/etter.dns để mở etter.dns
- Thêm tên miền muốn giả mạo

```
54 # NOTE: IPv6 specific do not work because ettercap has been built without
55 #       IPv6 support. Therefore the IPv6 specific examples has been
56 #       commented out to avoid ettercap throwing warnings during startup.
57 #
58 ##############################################################################
59 ###########
60 fb.com A 192.168.100.3
61 google.com A 192.168.100.3
62 ###########
63 # vim:ts=8:noexpandtab
```

3. Cấu hình website giả mạo

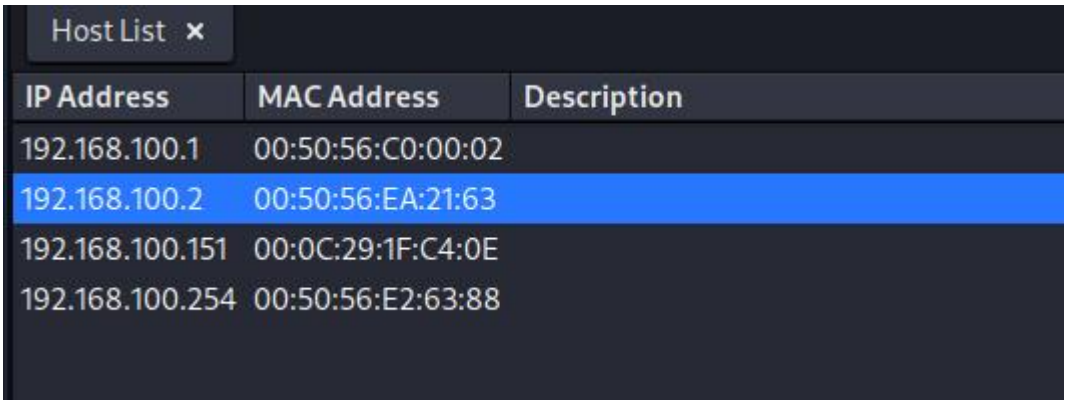
- Dùng lệnh nano index.html mở file /var/www/html/index.html và sửa đổi file

- Bật apache2

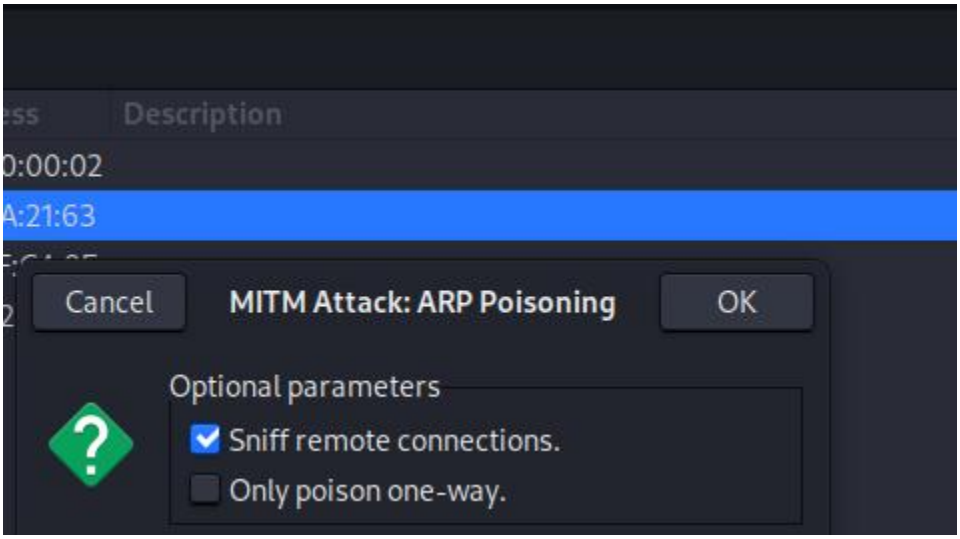
```
┌──(root㉿pmduc047)-[/home/kali]
└─# service apache2 restart

┌──(root㉿pmduc047)-[/home/kali]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disable>
     Active: active (running) since Fri 2023-09-22 18:58:37 EDT; 25s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 8826 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCES>
   Main PID: 8848 (apache2)
      Tasks: 6 (limit: 2277)
     Memory: 19.0M
        CPU: 938ms
     CGroup: /system.slice/apache2.service
             ├─8848 /usr/sbin/apache2 -k start
             ├─8850 /usr/sbin/apache2 -k start
             └─8851 /usr/sbin/apache2 -k start
```

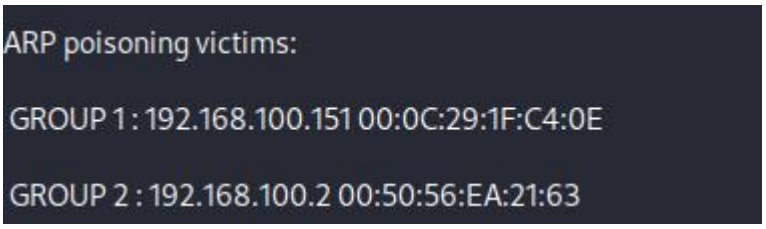
4. ***Mở Ettercap để tấn công (ettercap –G)***

– Scan host trong mạng phát hiện địa chỉ máy nạn nhân

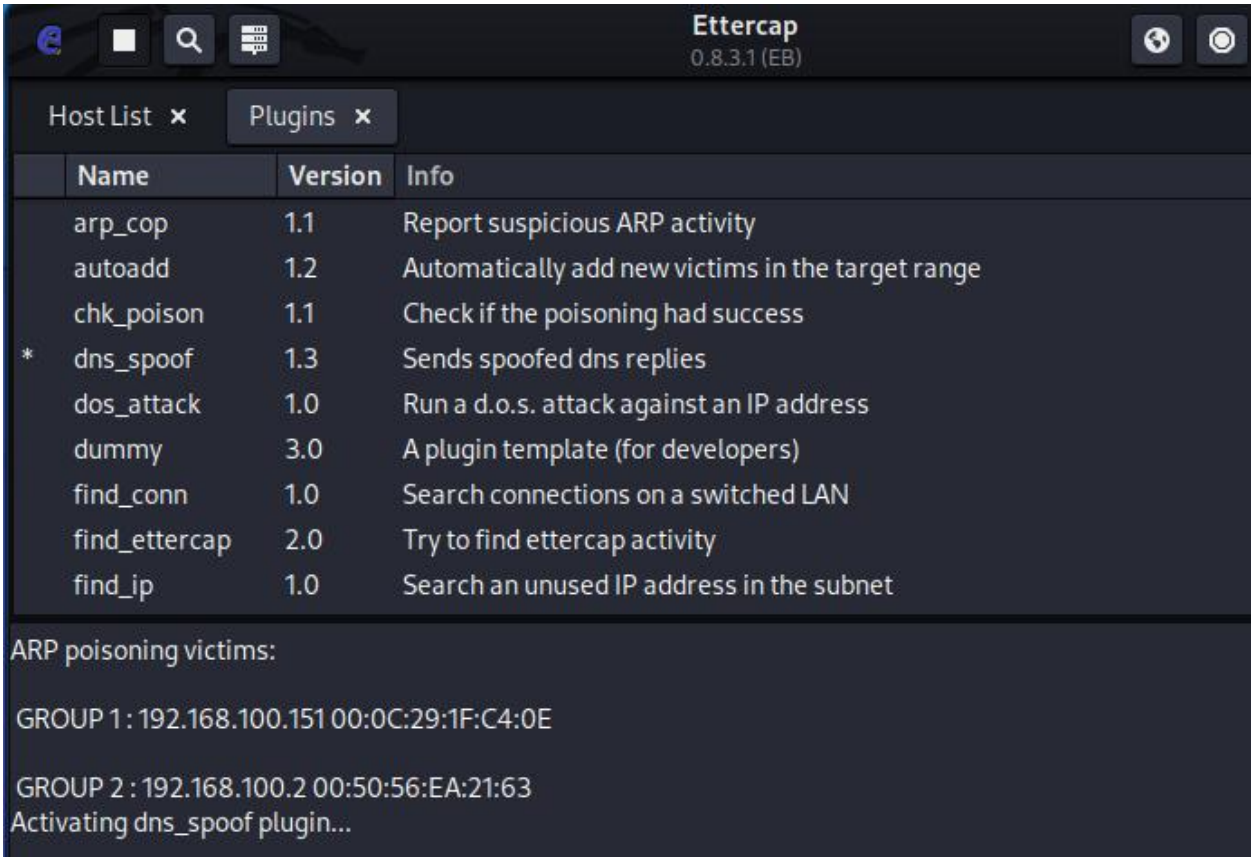


– Bắt đầu tấn công arp-poisoning



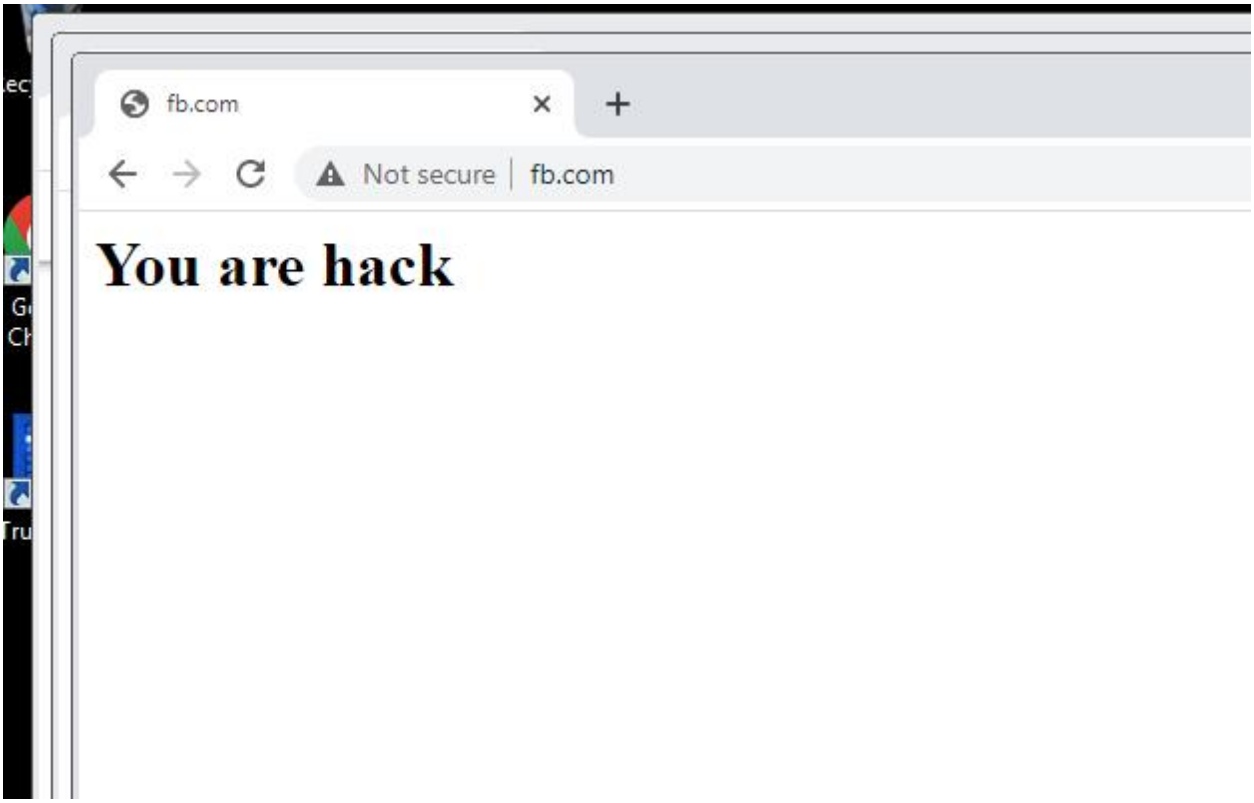


5. ***Sử dụng plugin dns spoofing khiến nạn nhân trực tiếp request đến well giả***



6. Kết quả

– Đăng nhập vào máy client tìm kiếm fb.com và nó hiển thị website mà mình giả mạo



VIII. Kết luận

DNS là viết tắt của *"Domain Name System"* (Hệ thống Tên Miền), là một giao thức quan trọng trong hạ tầng Internet. Nó cung cấp một cách để ánh xạ các tên miền thành địa chỉ IP mà máy tính có thể hiểu.

DNS bao gồm nhiều thành phần quan trọng, bao gồm **DNS Client (Resolver)**, **DNS Recursor**, **Root Name Server**, **TLD Name Server**, **Authoritative DNS Server**, **Caching DNS Servers**, **Zone Files**, **Root Hints File.**

DNS sử dụng các loại bản ghi (record types) để ánh xạ tên miền với các giá trị cụ thể như địa chỉ IP, mail server, v.v. Một vài bản ghi ví dụ như **A Record, AAAA Record, CNAME Record**, **MX Record, NS Record (Name Server), v.v**

DNS hoạt động theo cơ chế chuyển yêu cầu của máy client tới các máy chủ theo hệ thống cấp bậc, cho đến khi tìm thấy địa chỉ đích và gửi lại về client.

DNS có nhiều ứng dụng quan trọng trong hệ thống Internet:

- Truy cập Website
- Gửi và nhận email
- Dịch vụ mạng khác

DNS cũng có một số lỗ hổng bảo mật tiềm ẩn:

- **Cache Poisoning**
- **DNS Spoofing**
- **Amplification Attacks**
- **Zone Transfer Attacks**
- **Lỗ hổng DNSSEC (DNS Security Extensions)**
- **Kỹ thuật Fast Flux**

Các dạng tấn công DNS phổ biến:

- ***DNS Spoofing/Cache Poisoning***
- ***DNS Amplification***
- ***DNS Tunneling***
- ***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.***
- ***Giả mạo hoặc thay đổi các bản ghi trong DNS.***

Một số giải pháp bảo mật DNS:

DNSSEC (Domain Name System Security Extensions) là tiêu chuẩn an toàn mở rộng cho hệ thống DNS để đảm bảo việc xác thực và toàn vẹn của dữ liệu trong thông tin trả lời truy vấn tên miền của hệ thống DNS. Ngoài việc sử dụng công nghệ DNSSEC thì bạn còn có thể bảo vệ DNS của mình bằng các giải pháp sau:

- ***Sử dụng DNS Forwarder DNS Forwarder***
- ***Sử dụng máy chủ DNS lưu trữ***
- ***Sử dụng DNS Advertiser DNS Advertiser (Trình quảng cáo)***
- ***Sử dụng DNS Resolver DNS Resolver (trình xử lý) là một máy chủ DNS***
- ***Bảo vệ bộ nhớ đệm DNS***
- ***Bảo mật kết nối bằng DDNS***
- ***Ngừng chạy Zone Transfer Zone Transfer (vùng chuyển đổi)***
- ***Sử dụng Firewall kiểm soát truy cập DNS***
- ***Cài đặt kiểm soát truy cập vào file hệ thống DNS***
- ***Anycast routing***

IX. Tài liệu tham khảo:

- https://www.navee.asia/kb/dns-la-gi-tim-hieu-cach-thuc-hoat-dong-va-lo-hong-bao-mat/
- https://fptcloud.com/dns-la-gi/
- https://vietnix.vn/dns-la-gi/
- https://wiki.matbao.net/dns-security-la-gi-dns-security-ngan-chan-cac-cuoc-tan-cong-nhu-the-nao/
- https://vietnetco.vn/giai-phap-bao-mat-dns-tang-cuong-an-ninh-he-thong-doanh-nghiep/6416.html