|  |  |
| --- | --- |
|  | |
| **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  **Cơ sở tại thành phố Hồ Chí Minh**  **---------------------------------------** | |
|  | |
| **Báo cáo đồ án** | |
| **Môn học: Thực tập cơ sở**  **Đề tài: Triển khai dịch vụ DNS đảm bảo an toàn thông tin (Trên Linux)** | |
| **Giảng viên :** | **Huỳnh Trọng Thưa, Huỳnh Thanh Tâm** |
| **Sinh viên thực hiện:** | **Võ Tiến Đạt(leader) - N19DCAT016**  **Hoàng Anh Nhàn - N19DCAT056**  **Đoàn Hồng Tiến - N19DCAT072**  **Nguyễn Cao Phong - N19DCAT060**  **Trần Đình Chiến - N19DCAT010** |
| **Lớp:** | **D19CQAT01-N** |
|  | |
| **TP. HỒ CHÍ MINH - 2021** | |

**Danh mục hình ảnh, bảng, sơ đồ**

Hình 1: phân giải tên miền thành địa chỉ IP

Hình 2: phân giải địa chỉ IP thành tên máy

Hình 3: DNS Amplication Attack

Hình 4: Triển khai DNS Load Balancing

Hình 5: Round robin

Hình 6: Weight round robin

Hình 7 đến Hình 7.4: Cấu hình DNS server trên Centos7

Hình 7: sau đó cấu hình file /etc/named.conf

Hình 8: thêm forward zone vs reverse zone

Hình 9: cấu hình file forward.nhom6.local

Hình 10: cấu hình file reverse.nhom6.local

Hình 11: kiểm tra nslookup

Hình 12 : mô hình load balancing

Hình 13:Tiến hành cấu hình file /etc/haproxy/haproxy.cfg

Hình 14: kiểm tra loadbalancing

Hình 15 : mô hình tấn công

Hình 16: Địa chỉ IP máy victim

Hình 17: arp của máy victim

Hình 18:Xem địa chỉ IP máy attacker

Hình 19: Chạy ettercap trên máy attacker

Hình 20: Chọn Interface eth0 sau đó chọn Accept (dấu tích góc trên bên phải)

Hình 21: Chọn 1 để scan các máy có trong mạng, chọn 2 để xem danh sách

Hình 22: Lần lượt add to target default gateway của máy nạn nhân và ip nạn nhân

Hình 23: Chọn ARP poisoning

Hình 24: Chọn Sniff remote connections

Hình 25: Bảng ARP của nạn nhân trước và sau khi bị ARP poisoning

Hình 26: Mở Wireshark và chọn interface eth0 để bắt các gói tin

Hình 27: Bắt các gói tin của nạn nhân

Hình 28: Máy nạn nhân truy cập vào trang vnpost.vn và đăng nhập

Hình 29: Tìm kiếm mục đăng nhập dùng phương thức POST giao thức HTTP, đến đúng địa chỉ của vnpost.vn

Hình 30: Chọn Follow -> TCP Stream

Hình 31: Tìm ra User và password

Hình 32: mô hình DAI

Hình 33 : Cấu hình IP cho Server2

Hình 34: Cấu hình DHCP server cho Server2

Hình 35: Cấu hình IP cho Server3

Hình 36: Cấu hình DHCP server cho Server3

Hình 37: PC2 yêu cầu DHCP nhận IP thuộc lớp 192.168.0.0/24

Hình 38: PC2 yêu cầu DHCP nhận IP thuộc lớp 172.16.0.0/24

Hình 39: Xem nội dung bảng DHCP snooping bingding của Switch1

**Hình 40: Mô hình tấn công DDOS(https://www.digistar.vn/tan-cong-tu-choi-dich-vu-dos-va-ddos-phan-1/)**

Hình 41: Cài đặt bind9 để thiết lập máy chủ DNS

Hình 42: Kiểm tra IP của máy Ubuntu

Hình 43: Chỉnh sửa file cấu hình /etc/bind/named.conf.options

Hình 44: Chỉnh forwarders

Hình 45: Chỉnh sửa file cấu hình /etc/bind/named.conf.local

Hình 46: Thêm zone mới

Hình 47: Copy file /etc/bind/db.local qua /etc/bind/nhanhoanganh.vn.fw

Hình 48: Chỉnh sửa file /etc/bind/nhanhoanganh.vn.fw

Hình 49: Cấu hình lại /etc/bind/nhanhoanganh.vn để nhận IP của DNS Server

Hình 50: Copy file /etc/bind/db.127 qua /etc/bind/nhanhoanganh.vn.rv

Hình 51: Chỉnh sửa file /etc/bind/db.10

Hình 52: Cấu hình lại file /etc/bind/nhanhoanganh.vn.rv

Hình 53 : Chỉnh sửa file /etc/resolv.conf

Hình 54 : Kết quả phân giải thành công

Hình 55: Cài đặt Apache cho máy Ubuntu dung làm DNS Server

Hình 56: Cài đặt FirewallD

Hình 57: Mở port 80 và port 443 trên máy DNS Server để các máy khác trong mạng LAN có thể truy cập đến website của máy DNS Server

Hình 58: Cài đặt thành công có thể truy cập vào website mặc định của Apache trên DNS Server

Hình 59: Máy thật mang IP 192.168.85.5 đã truy cập được website từ DNS Server

Hình 60: Máy Kali (Hacker) DDOS bằng flood

Hình 61: Máy Windows 10 đã không còn truy cập được vào website từ DNS Server

**Lời mở đầu**

Trong thời đại ngày nay, vài trò internet vô cùng quan trọng. Điều này kéo theo ngành kinh tế, nhiều hoạt động chính trị, văn hóa phụ thuộc vào máy tính và internet. Chính vì vậy, ngày càng có nhiều ý đồ phá hoại nhằn vào hệ thống máy tính. Nhiều Website của các doanh nghiệp, tổ chức, công ty bảo mật hàng đầu thế giới đều bị hacker tấn công gây tổn thất lớn về tài chính và uy tín doanh nghiệp. Hình thức tấn công của hacker liên tục thay đổi và có nhiều cuộc tấn công của giới tối phạm công nghệ cao vào các hệ thống của doanh nghiệp và Chính phủ. Và em chọn đề tài “Triển khai dịch vụ DNS đảm bảo an toàn thông tin” để nghiên cứu. Mục tiêu của nhóm em là hiểu hơn về dịch vụ DNS và hiểu được các cuộc tấn công DNS thường gặp để có những kiến thức về an toàn thông tin trên không gian mạng.

Theo lời ông Bùi Duy Khánh, Trung tâm an ninh mạng FPT IS ở báo “khoa học và đời sống”: “Những người làm an toàn thông tin trên thế giới chấp nhận thực rằng không có hệ thống nào an toàn 100% mà chỉ có hệ thống biết mình bị tấn công và hệ thống không biết mình bị tấn công.”. Và có quá nhiều cuộc tấn công ngày này không thể nói hết trong một ngày hay hai ngày, vì vậy bài báo cáo của nhóm em chỉ trình bày ở những mức độ mà những cuộc tấn công phổ biến và cơ bản ngày nay nhiều người còn sử dụng để có mục đích xấu. Để hiểu đó là những cuộc tấn công nào và cần nắm những kiến thức gì mong mọi người tiếp theo dõi những phần trình bày của nhóm em sau đây.

**Chương I: Cơ Sở Lý Thuyết**

* **Tổng quan về dịch vụ DNS**
  1. **Giới thiệu về dịch vụ DNS**

DNS( domain Name System) được phát minh vào năm 1984 cho internet, là hệ thống phân giải tên chỉ một hệ thống phần giải tên chỉ một hệ thống đặt tên theo thứ tự cho dịch vụ, máy vi tính hay bất kì nguồn lực nào tham gia vào internet. Nó liên kết đa dạng các thông tin với tên miền được gán cho những người tham gia. Đặc biệt, nó chuyển tên miền có ý nghĩa cho con người vào số định danh, liên kết với những trang thiêt bị mạng cho các mục đích định vị và địa chỉ hóa thiết bị trên toàn cầu.

* 1. **Các bản ghi DNS**

Các bản ghi DNS phổ biến hiện nay:

* SOA( Start of Authority)
* NS (name server)
* Record A
* Record AAAA
* Record PTR
* Record SRV
* Record CNAME
* Record MX
* Record TXT
* Record DKIM
* Record SPF

Ví dụ về từng bản ghi hiện nay:

* SOA (Start of Authority)

Mỗi tập tin cơ sở dữ liệu DNS phải có một và chỉ một record SOA. Bao gồm thông tin về zone transfer

* NS (Name Server)

Record tiếp theo cần có trong zone là NS(name server) record. Mỗi name server cho zone sẽ có một NS record. Chứa địa chỉ IP của DNS Server cùng với các thông tin về domain đó

* Record A

Dùng để ánh xạ từ một domain thành địa chỉ IP cho phép có thể truy cập website.

Ví dụ

Cloud365.vn A 103.101.161.201

Tên miền con

Sub.cloud365.vn A 103.101.161.201

* Record AAAA

Dùng để ánh xạ một domain thành địa chỉ IPv6 cho phép truy cập website

* Record PTR

Có chức năng chuyển đổi IP sang tên miền.

* Record SRV
* Record CNAME
* Record MX
* Record TXT
* Record DKIM
* Record SPF
  1. **Cơ chế phân giải**
     1. **Phân giải tên miền thành địa chỉ IP**



Hình 1: Mô hình phân giải tên thành IP nguồn từ cloundflare.com

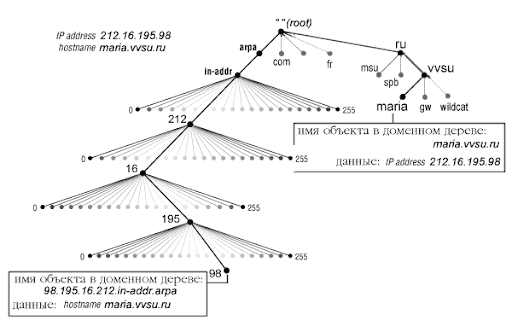
Khi có một client nào đó yêu cầu phân giải một domain thành IP thì đầu tiên yêu cầu được gửi đến DNS resolver, server này để tiến hành tìm kiếm trong bộ nhớ cache xem có IP tương ứng với domain đó không. Nếu không có sẽ yêu cầu đến Root DNS server, Root DNS server ( đây là server quan trọng nhất trong hệ thống cấp bậc của DNS), server này sẽ giúp Resolver tìm kiếm IP bằng cách sẽ chuyển hướng Resolver đến TLD server (server này quản lí các top-level: domain vd: .com, .net, . vn…)

Sau khi tìm được top-level domain. Server này sẽ tiếp tục chuyển hướng Resolver đến server cuối cùng, nơi diễn ra quá trình phân giải domain được gọi là Authoritative nameserver ( nơi chứa nguồn dữ liệu của domain đó, là nơi chứa một bảng mapping, nó map domain name với IP tương ứng). Sau đó nó sẽ đưa cho Resolver địa chỉ IP đã tìm thấy. Việc còn là là Resolver trả lời truy vấn cho phía client

* + 1. **Phân giải địa chỉ IP thành tên máy**

Cấu trúc của tên miền ngược (DNS reverse) như sau: [www.zzz.yyy.xxx.in-addr-arpa](http://www.zzz.yyy.xxx.in-addr-arpa). Trong đó: xxx, yyy, zzz, www là các số viết trong hệ thập phân biểu diễn giá tri của 4 byte cấu thành địa chỉ IP

Miên in-addr.arpa có thẻ có 256 subdomain. Tương ứng 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong đó mỗi Subdomain lại có 256 subdomain còn nữa ứng với byte thứ 2. Cứ như thế và đến byte thứ 4 có các bản ghi cho tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ IP tương ứng.



Hình 2: Mô hình phân giải IP thành tên

Lưu ý: khi đọc tên miền địa chỉ IP sẽ xuất hiện theo thứ tự ngược. Vì dụ nếu địa chỉ Ip của máy maria.vvsu.ru là 212.16.195.98, khi ánh xạ vào miền in-addr.arpa sẽ là 98.195.16.212. in-addr.arpa

* 1. **Phân quyền và bảo mật**

Ủy quyền: có nghĩa là chủ sở hữu domain mang lại toàn quyền kiếm soát nhánh cho người khác.

VD: chủ sở hữu là TLD server sau khi tìm được top-level-domain (.com), server này sẽ ủy quyền lại cho Authoritative name server thực hiện phân giải tên miền phụ yahoo.com chẳng hạn thành IP. Thì tại đây Server này sẽ làm bất cứ điều gì mà mình muốn không cần phải hỏi lại chủ sở hữu .com nữa.

Bảo mật: Hầu hết các cuộc tấn công này đều tập trung vào việc lạm dụng DNS để ngăn người dùng Internet không thể truy cập vào một số trang web nhất định. Chẳng hạn như các cuộc tấn công DNS spoofing/ cache poisoning ( đánh vào điểu yếu là DNS Resolver lưu các IP vào bộ nhớ cache), DNS tunneling, DNS hijaking… vv

Khắc phục: Sử dụng giao thức DNS security Extensions ( DNS SEC), giao thức này giúp bảo vệ cũng như chống lại các cuộc tấn công bằng cách sử dụng chữ ký điện tử vào các dữ liệu, giúp bảo vệ tính hợp lệ của nó. Để đảm bảo việc tìm kiếm an toàn, việc ký phải diễn ra mọi cấp trong quy định DNS lookup. Từ đó đảm bảo data không bị giả mạo. Ngoài ra cón cái công cụ như: DNS firewall

* **Tấn công DNS**
  1. **DNS spoofing (DNS cache poisoning)**
     1. **DNS spoofing và DNS poisoning**

Domain Name System (DNS) poisoning và spoofing là các loại cyberattack (tấn công mạng) phổ biến hiện nay. Chúng khai thác các lỗ hổng của DNS server để chuyển hướng lưu lượng truy cập từ các server hợp pháp sang các server giả mạo. Khi bạn đã truy cập vào một trang lừa đảo, bạn có thể bối rối về cách giải quyết nó. Bạn sẽ cần biết chính xác cách thức hoạt động của nó để tự bảo vệ mình.

DNS spoofing và DNS cache poisoning là một trong những cyberthreat lừa đảo phổ biến. Nếu không hiểu cách internet kết nối bạn với các trang web, bạn có thể bị lừa khi nghĩ rằng chính một trang web đã bị hack. Trong một số trường hợp, có thể là chính thiết bị của bạn vừa bị hack. Tệ hơn nữa, các bộ cybersecurity hiện nay chỉ có thể ngăn chặn một số mối đe dọa liên quan đến DNS spoof.

* + 1. **Cách hoạt động của DNS Cache Poisoning và Spoofing**

Liên quan đến DNS, đây là 2 mối đe dọa nổi bật nhất:

DNS spoofing: bắt chước các điểm đến của server hợp pháp để chuyển hướng lưu lượng truy cập của domain. Các nạn nhân không nghi ngờ gì sẽ truy cập vào các trang web độc hại. Đó cũng là mục tiêu của DNS spoofing.

DNS cache poisoning là một phương pháp DNS spoofing phía user. Trong đó, hệ thống của bạn log địa chỉ IP giả trong local memory cache. Điều này dẫn đến việc DNS sẽ recall trang web xấu. Ngay cả khi sự cố đã được giải quyết hoặc chưa bao giờ tồn tại ở phía server.

* + 1. **Các phương pháp tấn công DNS Spoofing hoặc Cache Poisoning**

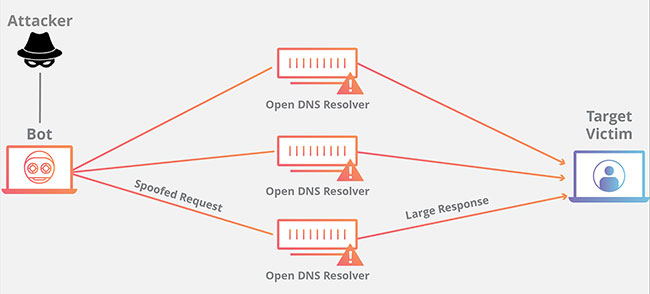
Có nhiều phương pháp để tấn công DNS Spoof, sau đây là một số phương pháp phổ biến:

Man-in-the-middle duping: Nơi kẻ tấn công nằm giữa web browser của bạn và DNS server để lây nhiễm cả hai. Một tool được sử dụng để tấn công cache poisoning đồng thời trên cả thiết bị local của bạn và server poisoning trên DNS server. Kết quả là chuyển hướng đến một trang web độc hại được host trên local server của chính kẻ tấn công.

DNS server hijack: Tội phạm trực tiếp cấu hình lại server để hướng tất cả request của user đến trang web độc hại. Khi DNS entry giả được đưa vào DNS server, bất kỳ IP request nào cho spoofed domain sẽ dẫn đến trang web giả mạo.

DNS cache poisoning via spam: Code của DNS cache poisoning thường được tìm thấy trong các URL được gửi qua email spam. Những email này cố gắng khiến user sợ hãi khi nhấp vào URL được cung cấp. Từ đó lây nhiễm vào máy tính của họ. Bên cạnh đó, quảng cáo biểu ngữ và hình ảnh cả trong email và các trang web không đáng tin cậy cũng có thể hướng user đến code này. Sau khi bị poisoned, máy tính của bạn sẽ đưa bạn đến các trang web giả được giả mạo để trông giống như thật. Đây là nơi các mối đe dọa thực sự sẽ xâm nhập vào thiết bị của bạn.

* 1. **DNS Amplication Attack**



**Hình 3:** DNS Amplication Attack

DNS Amplification, giống như các cuộc tấn công khuếch đại khác, là loại tấn công phản chiếu. Trong trường hợp này, việc phản chiếu đạt được bằng cách gợi ra phản hổi từ trình phân giải DNS tời một địa chỉ IP giả mạo

Trong một cuộc tấn công DNS Amplification, thủ phạm sẽ gửi một truy vấn DNS có địa chỉ IP giả mạo ( của nạn nhân) tới một trình phần giải DNS đang mở, khiến nó trả lời lại địa chỉ đó bằng cách phản hồi DNS. Với nhiều truy vấn được gửi đi và trình phân giải DNS trả lợi lại đồng thời, mạng của nạn nhận có thế dễ dàng

* **Các phương pháp bảo mật đối với DNS**

**3.1 Cách ngăn chặn và ngăn ngừa DNS Cache Poisoning và Spoofing**

Đối với chủ sở hữu trang web và nhà cung cấp DNS server:

* Sử dụng các công cụ phát hiện DNS Poisoning
* Sử dụng các tiện ích bảo mật DNS Mã hóa end-to-end

Đối với endpoint user:

* Không bao giờ nhấp vào liên kết mà bạn không nhận ra
* Thường xuyên scan máy tính để tìm phần mềm độc hại Flush DNS cache của bạn để giải quyết vấn đề nhiễm độc
* Sử dụng virtual private network (VPN).

**3.2 Cách ngăn chặn tấn công DNS Amplification**

* Giữ cho trình phân giải ở chế độ riêng tư và được bảo vệ

Nếu bạn vận hành trình phân giải của riêng mình, việc sử dụng trình phân giải đó nên được giới hạn cho người dùng trên mạng của bạn để giúp ngăn bộ nhớ cache của nó bị nhiễm độc bởi tin tặc bên ngoài tổ chức. Nó không thể được mở cho người dùng bên ngoài.

Hãy cấu hình nó bảo mật nhất có thể để chống lại việc lây nhiễm phần mềm độc hại vào bộ nhớ cache. Các biện pháp bảo vệ được tích hợp trong phần mềm DNS bảo vệ chống lại việc lây nhiễm sang bộ nhớ cache bao gồm thêm tính năng thay đổi đối với các yêu cầu gửi đi, để khiến hacker khó nhận được phản hồi không có thật. Các cách có thể thực hiện điều này bao gồm:

* Sử dụng một cổng nguồn ngẫu nhiên (thay vì cổng UDP 53)

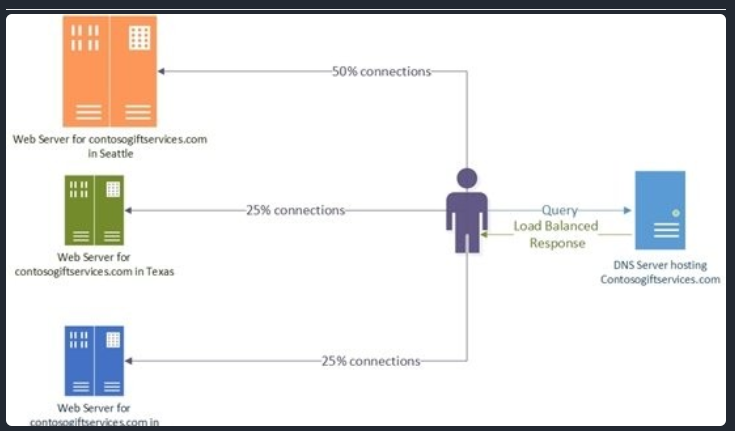
Ngẫu nhiên hóa ID truy vấn

Đặt ngẫu nhiên các chữ cái viết hoa, viết thường trong tên miền gửi đi để phân giải. (Đó là vì máy chủ định danh sẽ xử lý example.com và ExaMPle.com giống nhau khi phân giải địa chỉ IP, nhưng nó sẽ phản hồi bằng cách sử dụng cùng một kiểu viết như truy vấn ban đầu).

* Quản lý DNS server một cách bảo mật

Khi nói đến các máy chủ có thẩm quyền, bạn cần quyết định tự mình host chúng hay làm việc đó thông qua nhà cung cấp dịch vụ hoặc công ty đăng ký domain. Một chuyên gia nói rằng: “Không ai quan tâm đến bảo mật của bạn nhiều hơn chính bạn đâu, vì vậy bạn nên tự host và quản lý, nếu bạn có đủ kỹ năng để làm như vậy“.

**4. Triển khai DNS Load Balancing**



**Hình 4:** Triển khai DNS Load Balancing

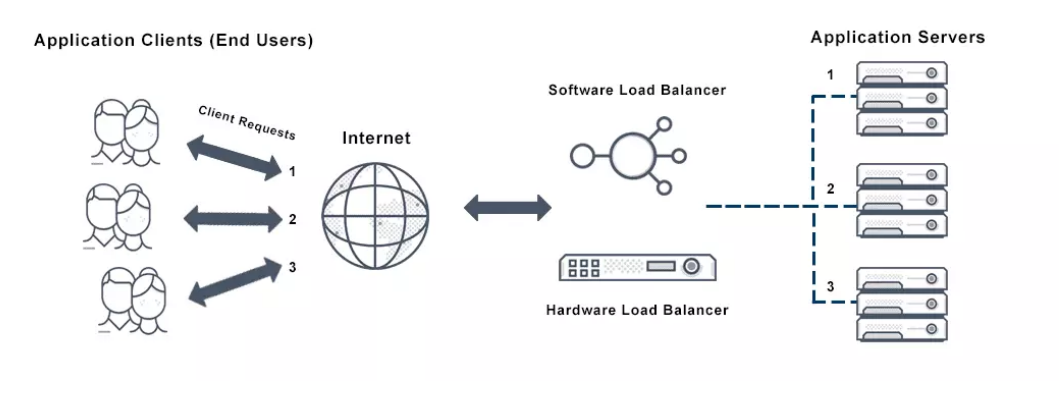
Load balancer dựa trên DNS thực sự là một trong những phương án thực hiên đơn giản nhất nếu có kinh nghiệm về quản trị hệ thống server, bằng cách thực hiện một cấu hình đơn giản trên máy chủ DNS. Nguyên tắc là khi người dùng truy cập một tên miền, trước tiên, nó sẽ phẩn giải địa chỉ IP tương ứng với tên miền cho máy chủ DNS. Tại thời điểm này có thể cho phép máy chủ DNS trả về các IP khác nhau theo người dùng ở các vị trí địa lí khác nhau

Ưu điểm: DNS làm giải pháp Load Balancer là cấu hình đơn giản và chi phí thực hiện rất thấp mà không cần thêm công việc phát triển và bảo trì

Nhược điểm: khi cấu hình DNS được sửa đổi, nó sẽ không có hiệu lực kịp thời. Điều này là do các đặc điểm của DNS. DNS thường có nhiều cấp độ cache, chính vì vậy khi chúng ta sửa đổi cấu hình DNS, cache chưa thay đổi kịp, thì dẫn tới việc IP sẽ không kịp thời cập nhật, do đó ảnh hưởng đến hiệu quả load balancer.

* Các thuật toán thường được dùng

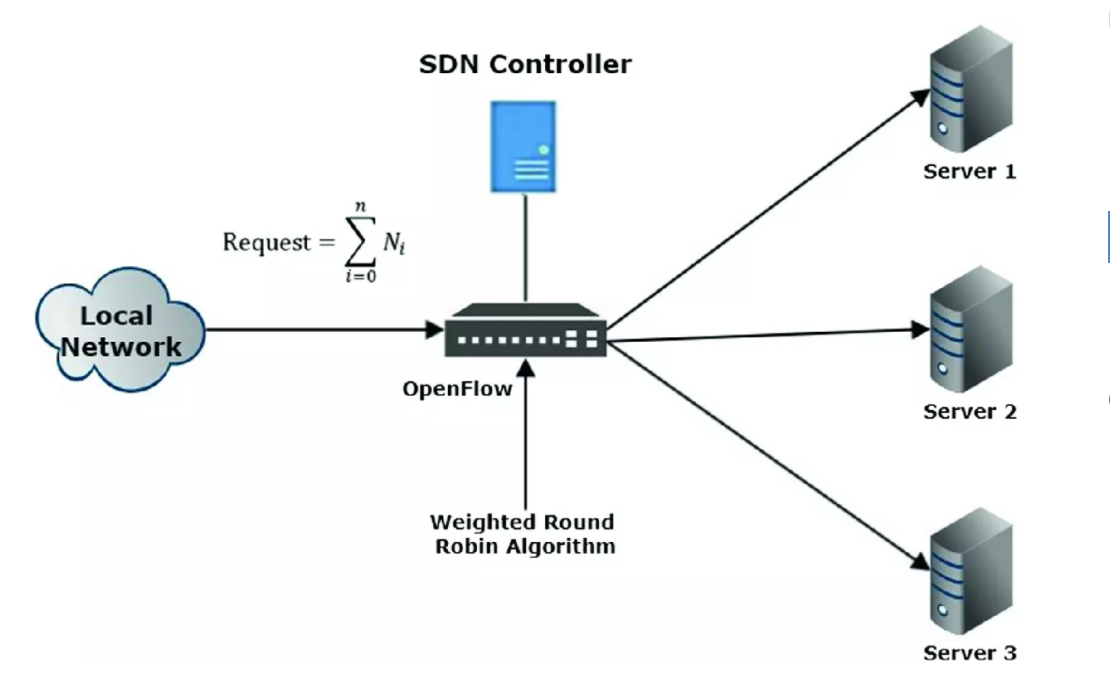
**Round robin**



**Hình 5:** Round robin

Dễ dàng để hiểu và triển khai, là thuật toán được sử dụng rộng rãi nhất. Request sẽ được chuyển hướng tới server theo vòng tròn. Thuật toán này hoạt động hiệu quả khi các server này có khả năng tính toán và lưu trữ giống nhau.

**+ Weight round robin**



**Hình 6:** Weight round robin

Đây là thuật toán mở rộng của thuật toán Round Robin. Đối với Round Robin, server phải xử lí khối lượng request là ngang nhau. Nếu 1 server có nhiều CPU, nhiều RAM hơn, thuật toán này cũng không thể phân phối nhiều request hơn cho server này được. Do đó, server với khả năng xử lí thấp hơn có thể sẽ bị overload và nhanh chóng quá tải trong khi server mạnh hơn thì đang nhàn rỗi.

Thuật toán Weighted Round Robin yêu cầu quản lý Admin cho việc chỉ định trọng lượng cho mỗi server dựa trên năng lực xử lý. Server nào có trọng lượng cao hơn thì nhận nhiều request hơn. Ví dụ:

* Server A có khả năng xử lý 15 request mỗi giây (tỉ lệ trung bình)
* Server B có khả năng xử lý 10 request mỗi giây (tỉ lệ trung bình)
* Server C có khả năng xử lý 5 request mỗi giây (tỉ lệ trung bình)

Giả sử có 6 request thì:

* 3 request được gửi tới server A
* 2 request được gửi tới server B
* 1 request được gửi tới server C

**+ Dynamic round robin**

Thuật toán DRR hoạt động gần giống với thuật toán WRR. Điểm khác biệt là trọng số ở đây dựa trên sự kiểm tra server một cách liên tục. Do đó trọng số liên tục thay đổi.

Việc chọn server sẽ dựa trên rất nhiều khía cạnh trong việc phân tích hiệu năng của server trên thời gia thực. Ví dụ: số kết nối hiện đang có trên các server hoặc server trả lời nhanh nhất, …

Thuật toán này thường không được cài đặt trong các bộ cân bằng tài đơn giản. Nó thường được sử dụng trong các sản phẩm cân bằng tải của F5 Network.

**+ Fastest**

Đây là thuật toán dựa trên tính toán thời gian đáp ứng của mỗi server (response time). Thuật toán này sẽ chọn server nào có thời gian đáp ứng nhanh nhất. Thời gian đáp ứng được xác định bởi khoảng thời gian giữa thời điểm gửi một gói tin đến server và thời điểm nhận được gói tin trả lời.

Việc gửi và nhận này sẽ được bộ cân bằng tải đảm nhiệm. Dựa trên thời gian đáp ứng, bộ cân bằng tải sẽ biết chuyển yêu cầu tiếp theo đến server nào.

Thuật toán Fastest thường được dùng khi các server ở các vị trí địa lý khác nhau. Như vậy người dùng ở gần server nào thì thời gian đáp ứng của server đó sẽ nhanh nhất. Cuối cùng server đó sẽ được chọn để phục vụ.

**+ Least connections**

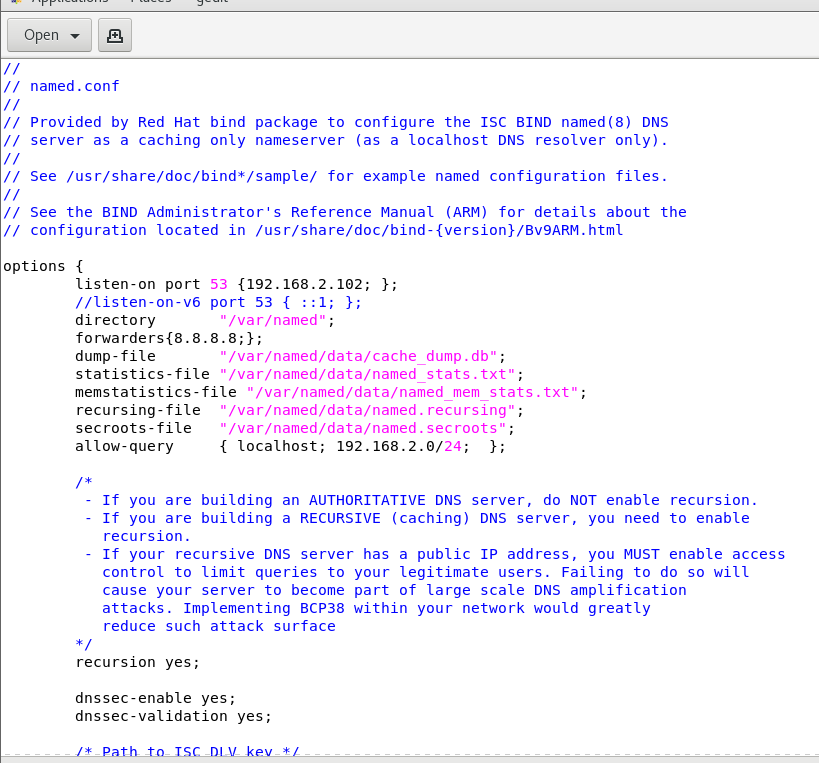
Các request sẽ được chuyển vào server có ít kết nối nhất trong hệ thống. Thuật toán này được coi như thuật toán động, vì nó phải đếm số kết nối đang hoạt động của server.

**Least Connections** có khả năng hoạt động tốt. Ngay cả khi tải của các kết nối biến thiên trong một khoảng lớn. Do đó nếu sử dụng RC sẽ khắc phục được nhược điểm của Round Robin.

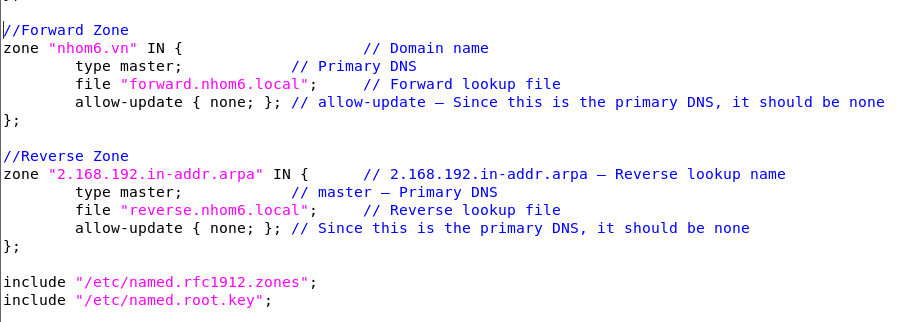
**Chương II: Thiết kế và xây dựng**

1. **Cấu hình DNS server trên Centos7**

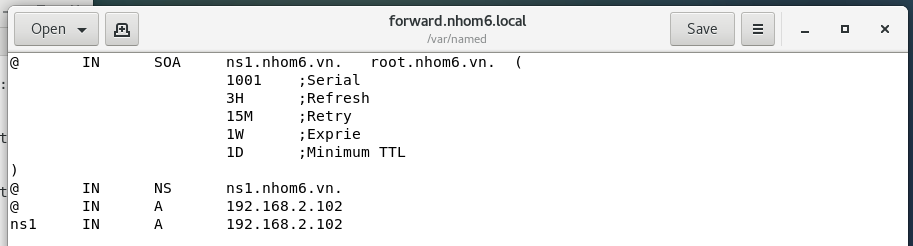
* Cài đặt bind9

****

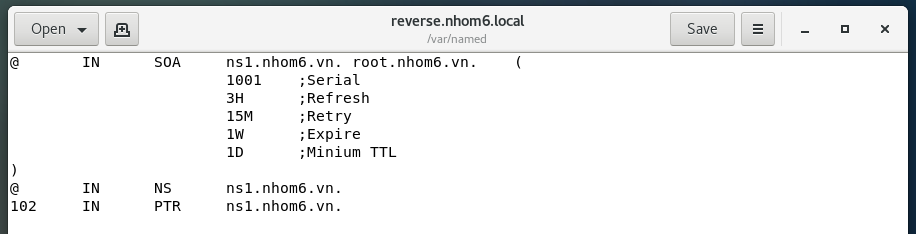
Hình 7: sau đó cấu hình file /etc/named.conf



Hình 8: thêm forward zone vs reverse zone

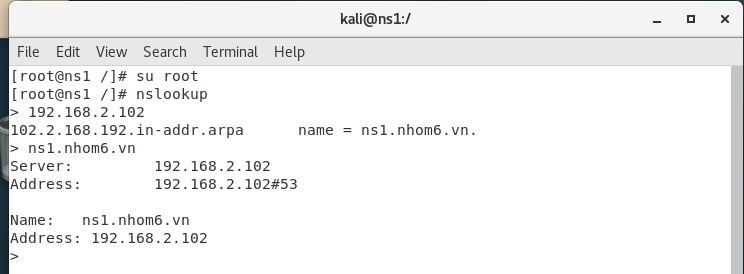


Hình 9: cấu hình file forward.nhom6.local



Hình 10: cấu hình file reverse.nhom6.local

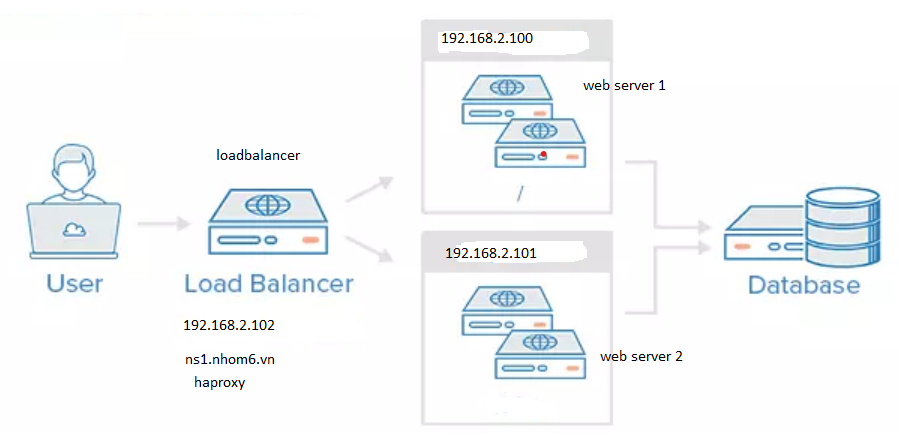
* Thêm port 53: firewall-cmd –permanent –add-port=53/tcp
* Restart lại name: systemctl restart named



Hình 11: kiểm tra nslookup

1. **Cấu hình load balancing**

**2.1 Mô hình**

****

Hình 12 : mô hình load balancing

* 1. **Cấu hình**
* Chuẩn bị 3 máy

|  |  |  |
| --- | --- | --- |
| **Máy loadbalancer** | **Máy web server 1** | **Máy web server 2** |
| IP: 192.168.2.102  GW: 192.168.2.1  DNS:192.168.2.102, 8.8.8.8 | IP: 192.168.2.100  GW: 192.168.2.1  DNS: 192.168.2.100 | IP: 192.168.2.101  GW: 192.168.2.1  DNS Server: 192.168.2.101 |

* Cài đặt apache2 trên hai máy webserver

**yum install httpd**

* Tiến hành mở port 80 trên hai máy web server

**firewall-cmd --permanent --add-port=80/tcpMột máy DC12-01**

* Tiến hành cài đặt haproxy trên máy load balancer



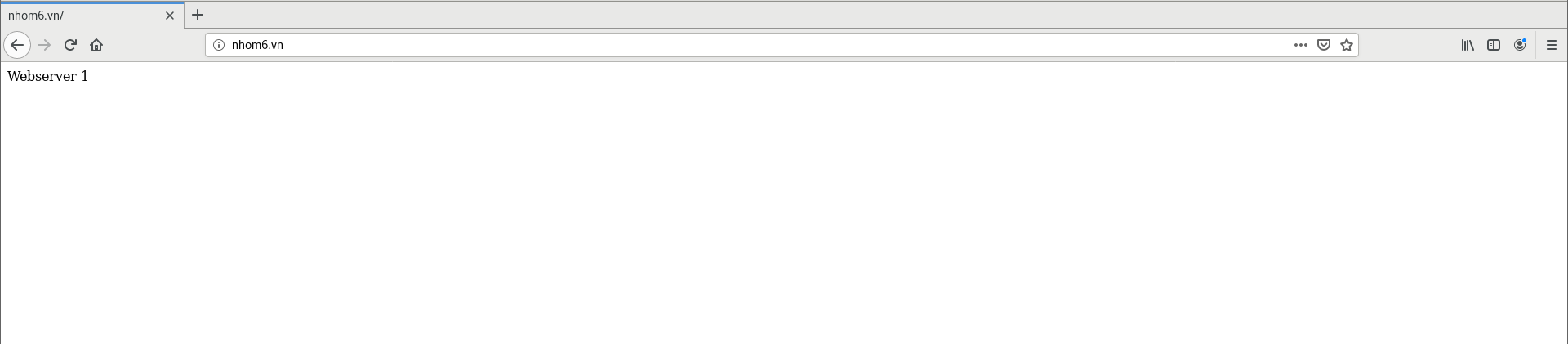
Hình 13:Tiến hành cấu hình file /etc/haproxy/haproxy.cfg

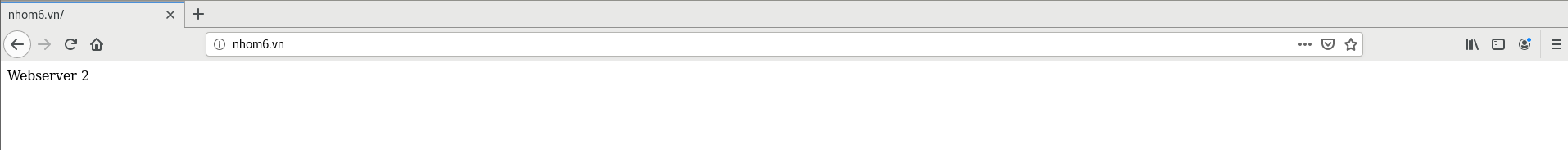
-Tiến hành enable vs start haproxy

**Systemctl enable haproxy**

**Systemctl start haproxy**

**-**Tiến hành kiểm tra

****

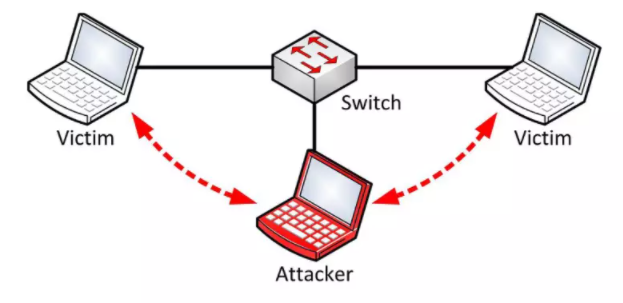
****

Hình 14: kiểm tra loadbalancing

**Chương III: Kết quả thực nghiệm**

**Kịch bản 1: Tấn công arp poisoning**

**Mô hình tấn công**

****

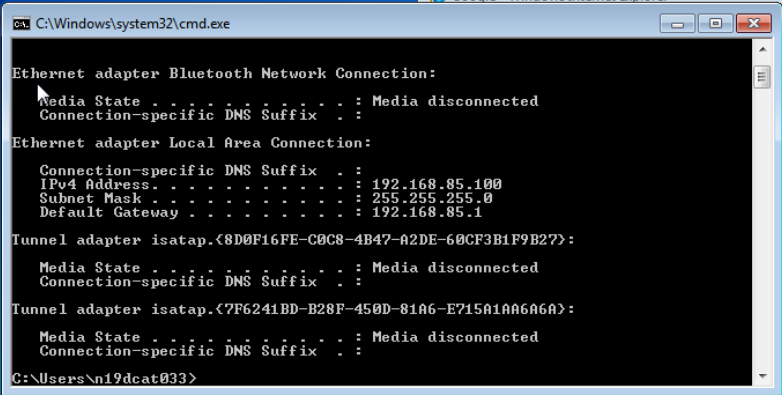
Hình 15 : mô hình tấn công

**Tấn công**

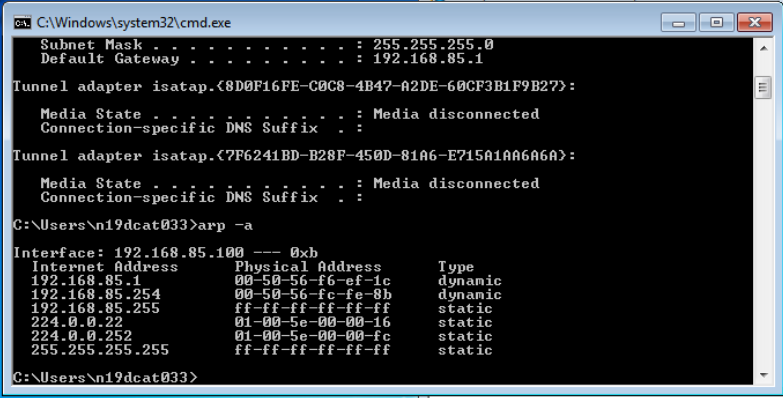
**2.1Chuẩn bị và kiểm tra trước khi tấn công**

|  |  |
| --- | --- |
| Máy attacker: | Victim: |
| IP address: 192.168.85.129  NETMASK: 255.255.255.0  DEFAULT GATEWAY: 192.168.85.1 | IP ADDRESS: 192.168.85.100  NETMASK: 255.255.255.0  DEFAULT GATEWAY: 192.168.85.1 |

Kiểm tra địa chỉ IP và arp ở máy victim

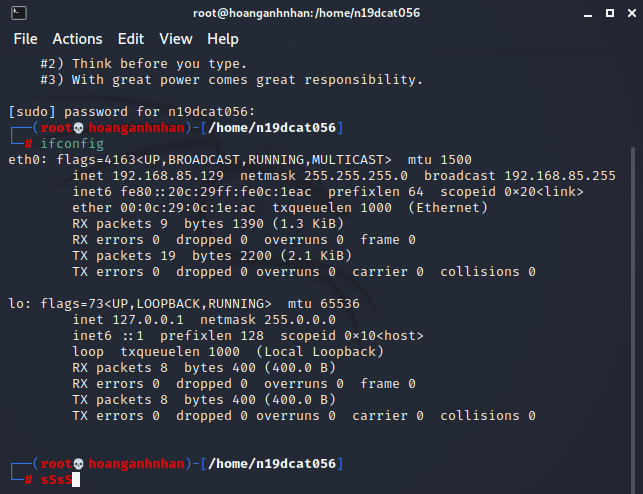


Hình 16: Địa chỉ IP máy victim



Hình 17: arp của máy victim

Kiểm tra IP của máy attacker

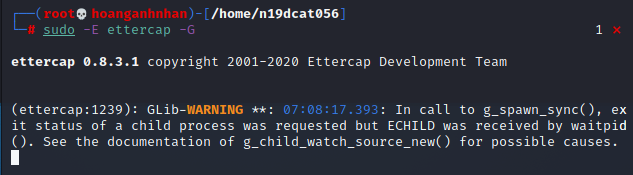


Hình 18:Xem địa chỉ IP máy attacker

**2.2Tấn công**

Chạy ettercap trong máy attacker

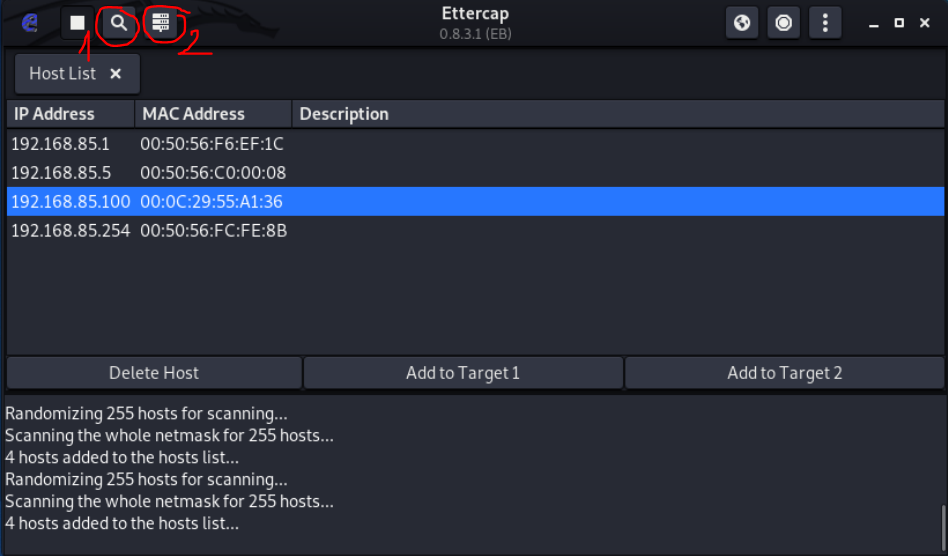
Sudo –E ettercap –G



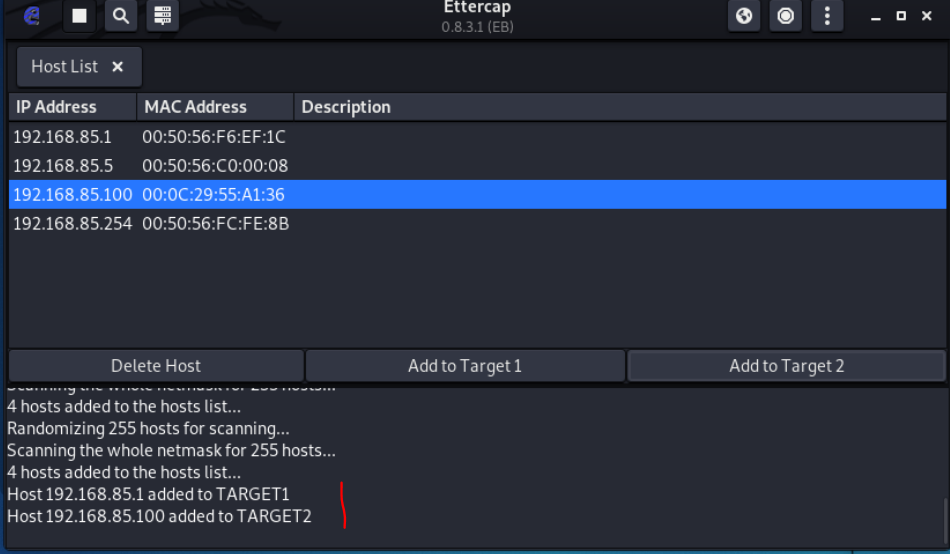
Hình 19: Chạy ettercap trên máy attacker



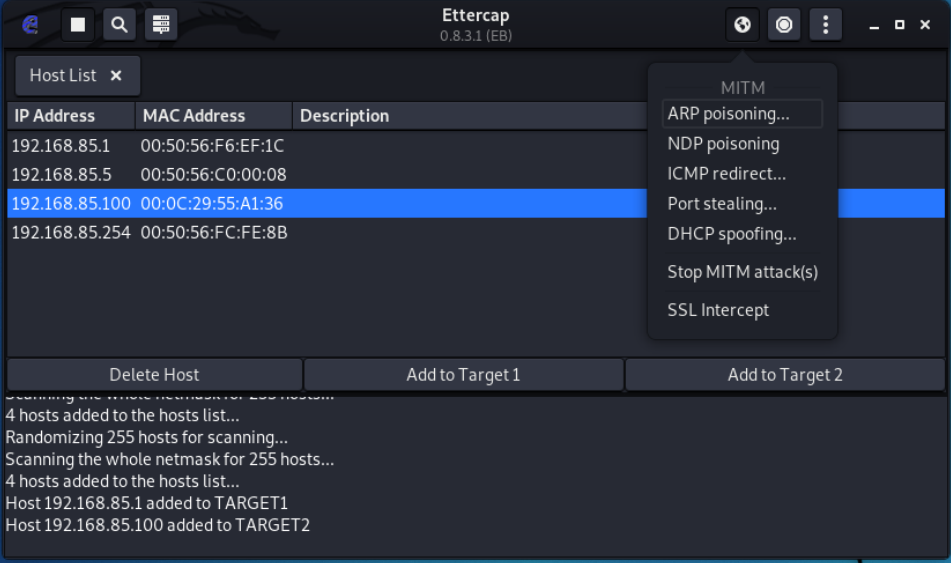
Hình 20: Chọn Interface eth0 sau đó chọn Accept (dấu tích góc trên bên phải)



Hình 21: Chọn 1 để scan các máy có trong mạng, chọn 2 để xem danh sách



Hình 22: Lần lượt add to target default gateway của máy nạn nhân và ip nạn nhân

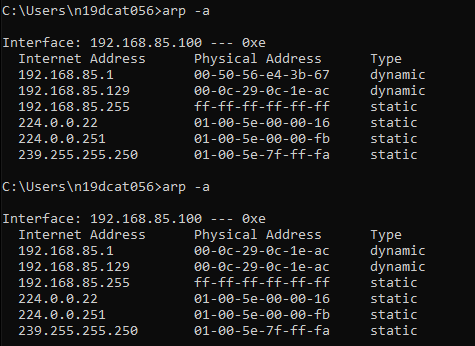


Hình 23: Chọn ARP poisoning

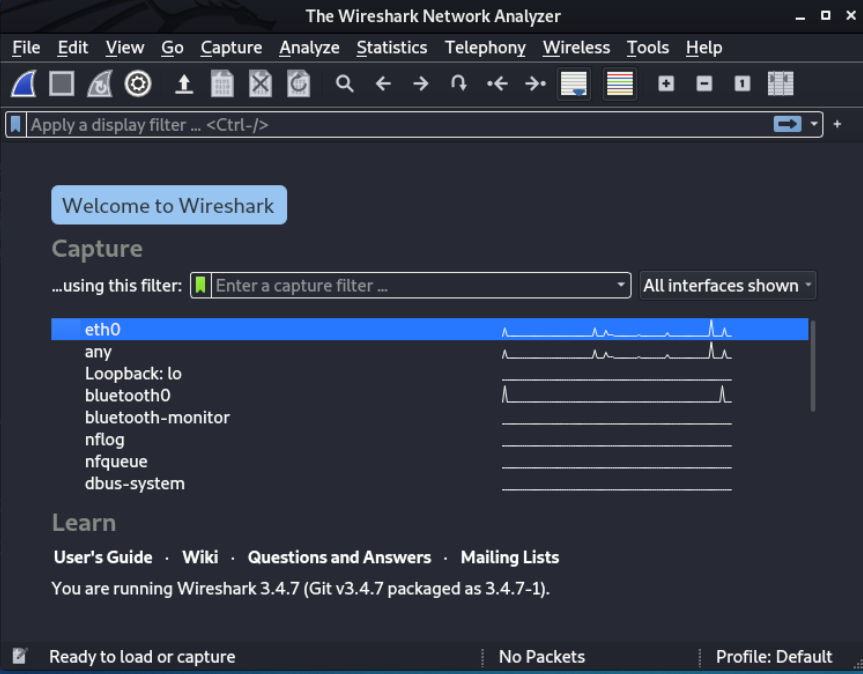


Hình 24: Chọn Sniff remote connections

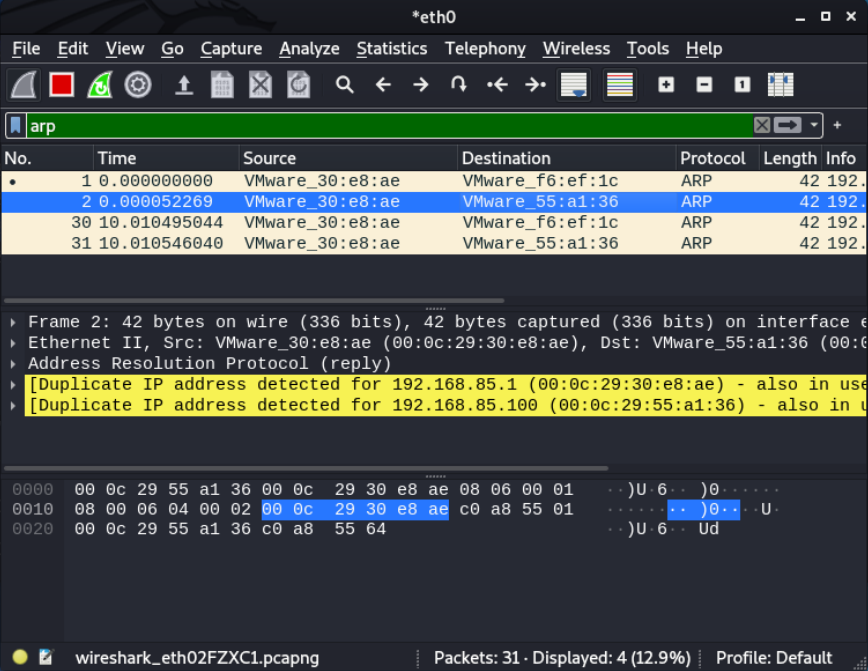
**2.3Kêt quả sau khi tấn công**



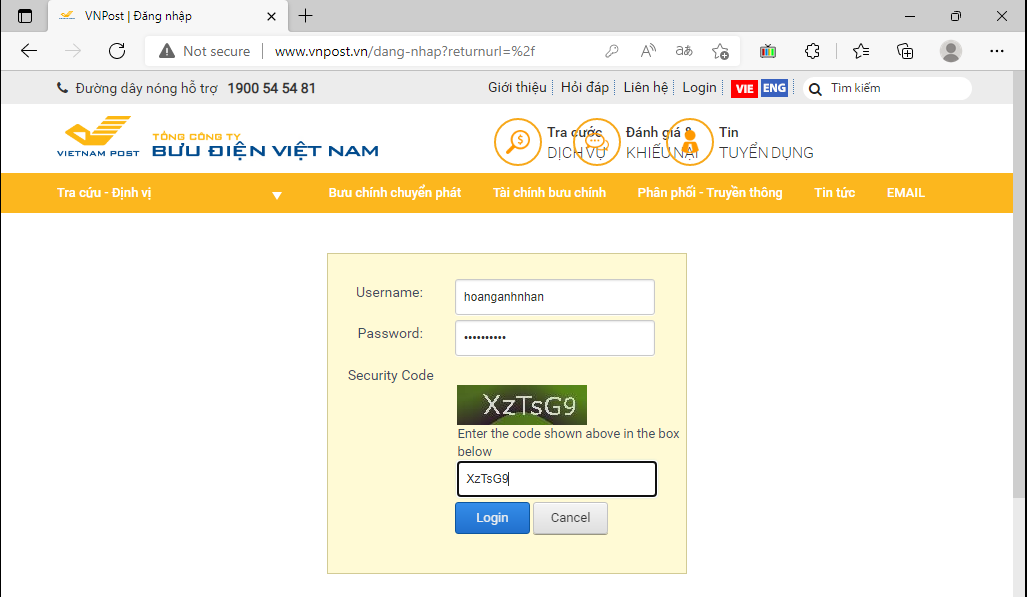
Hình 25: Bảng ARP của nạn nhân trước và sau khi bị ARP poisoning



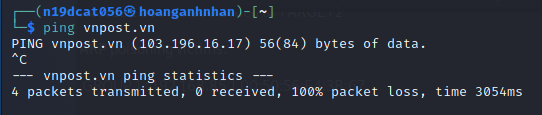
Hình 26: Mở Wireshark và chọn interface eth0 để bắt các gói tin



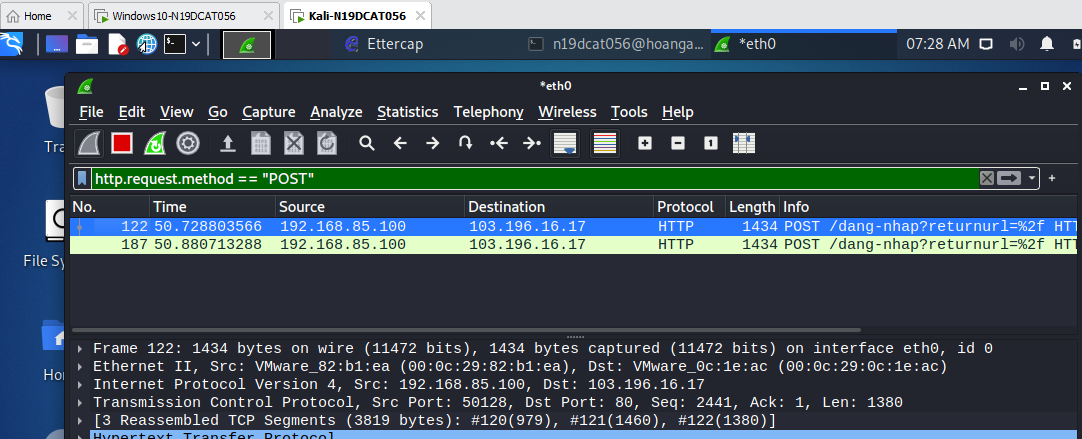
Hình 27: Bắt các gói tin của nạn nhân



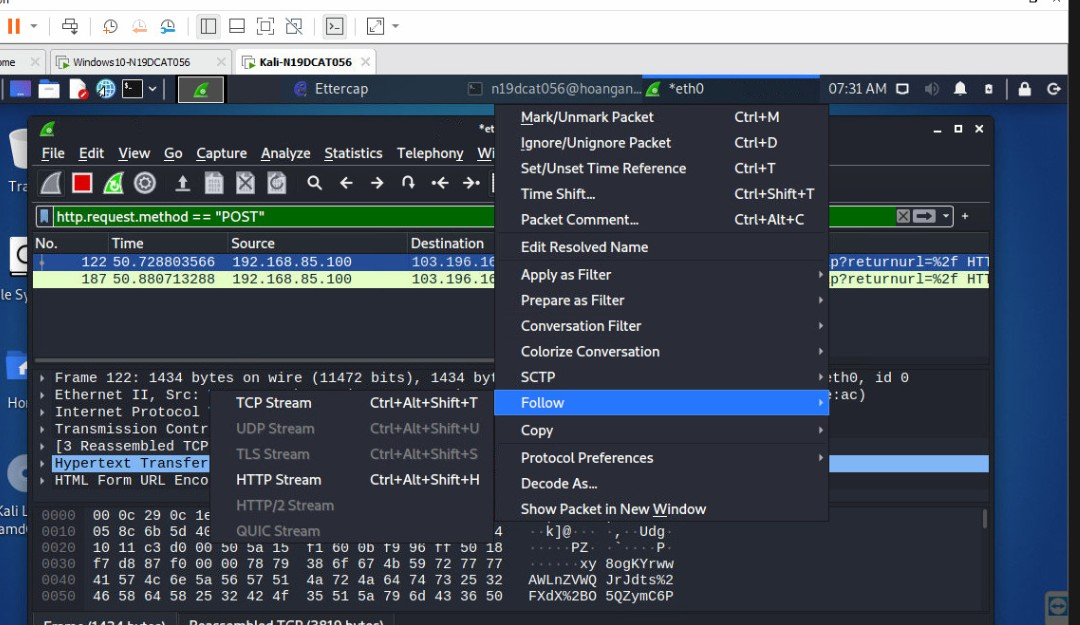
Hình 28: Máy nạn nhân truy cập vào trang vnpost.vn và đăng nhập



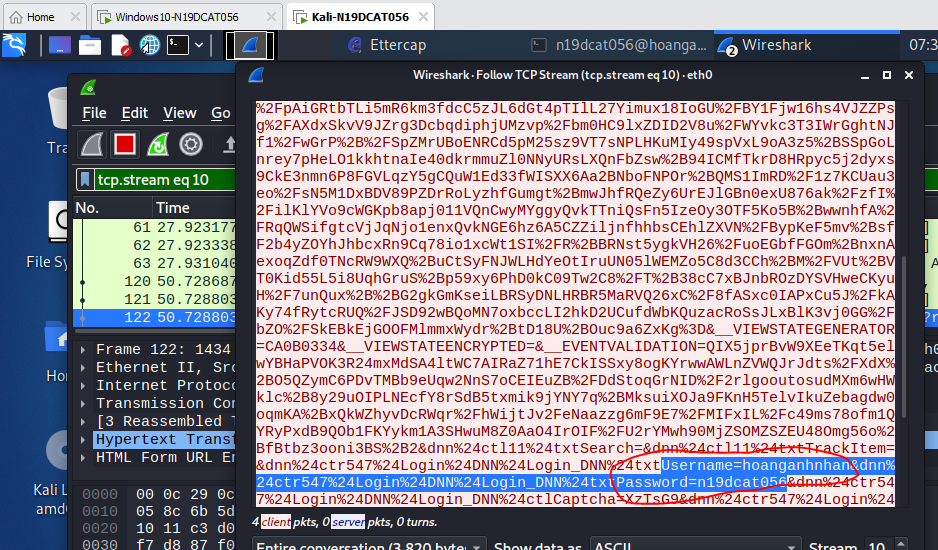
Hình 20: Kiểm tra địa chỉ của vnpost.vn



Hình 29: Tìm kiếm mục đăng nhập dùng phương thức POST giao thức HTTP, đến đúng địa chỉ của vnpost.vn



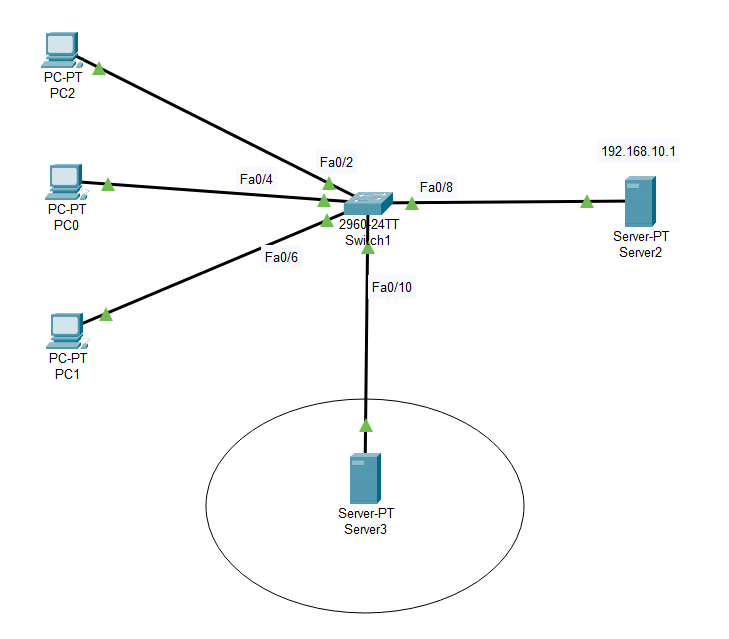
Hình 30: Chọn Follow -> TCP Stream



Hình 31: Tìm ra User và password

1. **Phòng thủ**

Mô hình



Hình 32: mô hình DAI

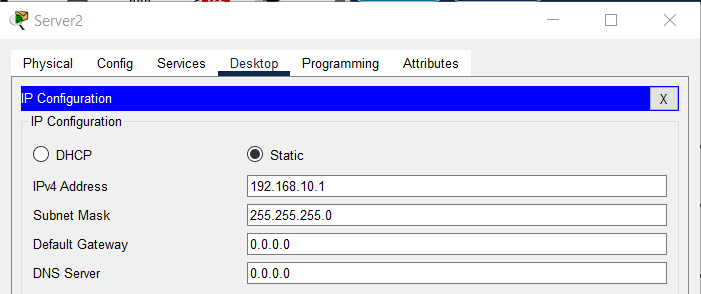
Quy Hoạt IP

|  |  |  |
| --- | --- | --- |
| **Tên Thiết Bị** | **IP** | **Chú Thích** |
| Server2 | 192.168.0.1 | Default Gateway của Vlan :  192.168.1.20  Start IP Address:  192.168.1.30 |
| Server3 | 172.16.0.1 | Default Gateway của Vlan :172.16.0.1  Start IP Address: 172.16.0.11 |
| Switch 1 | Interface vlan 1 | Cổng quản lý |
| PC0 | NIC: Xin DHCP |  |
| PC1 | NIC: Xin DHCP |  |
| PC2 | NIC: Xin DHCP |  |

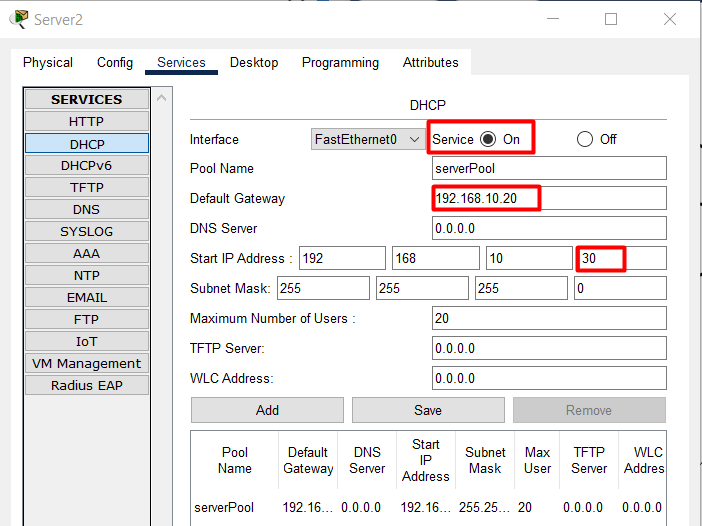
Mô tả hình thức tấn công:

1. Trên Switch1 tạo VLAN 1 và thực hiện kết nối các PC0, PC1, PC2, Server2, Server3 lần lượt Fast Ethernet 0/4, Fa0/2, Fa0/6, Fa0/8, Fa0/1
2. Cấu hình PC0,PC1,PC2 làm DHCP server cấp các IP thuộc lớp 192.168.0.0/24 và 172.16.0.0/24 VLAN 1
3. Cấu hình trên Switch1 tính năng DHCP Snooping cho VlAN 1
4. Cấu hình tính năng DAI trên các cổng thuộc VLAN 1 đảm bảo các user kết nối vào các cổng thuộc VLAN 1 phải sử dụng đúng địa chỉ MAC. Nếu thay đổi địa chỉ MAC thì không thể trao đổi dữ liệu thông qua Switch1 ( Cụ thể: chỉ ra cổng Fa0/8 chỉ được phép cấp DHCP)

Cấu hình Server2:

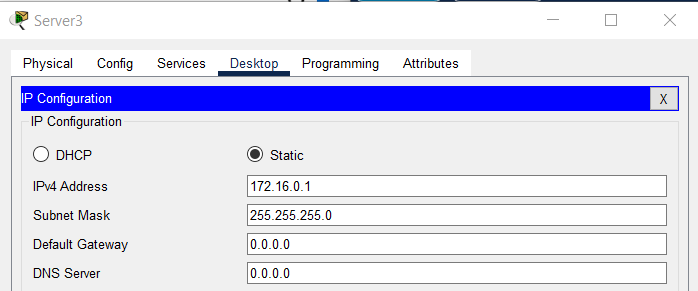


Hình 33 : Cấu hình IP cho Server2

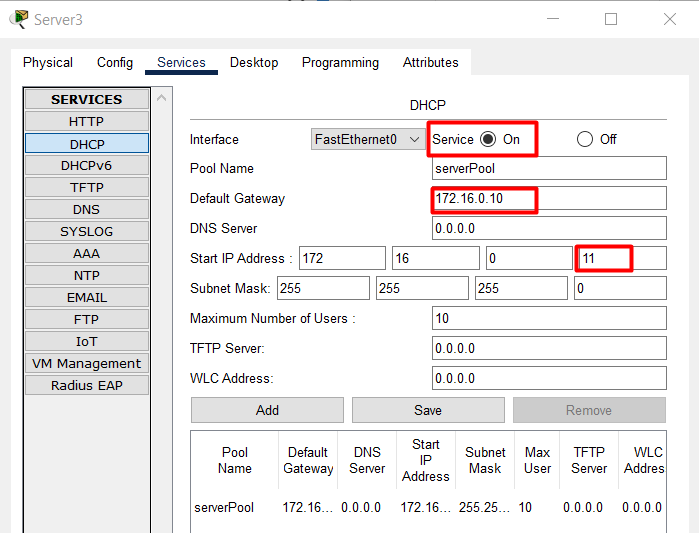


Hình 34: Cấu hình DHCP server cho Server2

Cấu hình Server3:



Hình 35: Cấu hình IP cho Server3

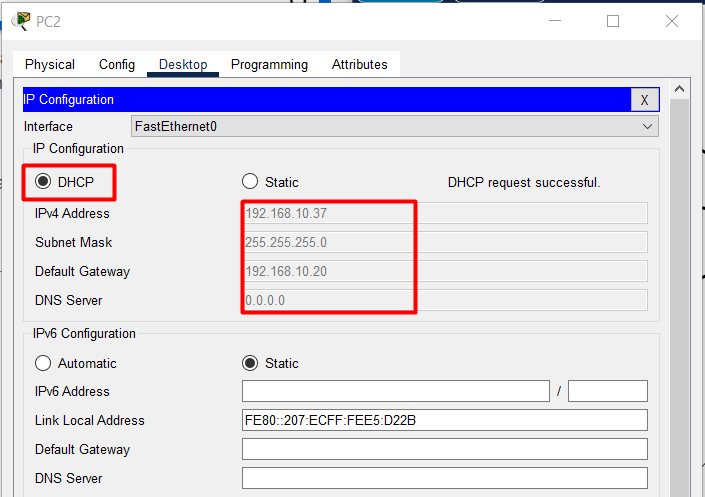


Hình 36: Cấu hình DHCP server cho Server3

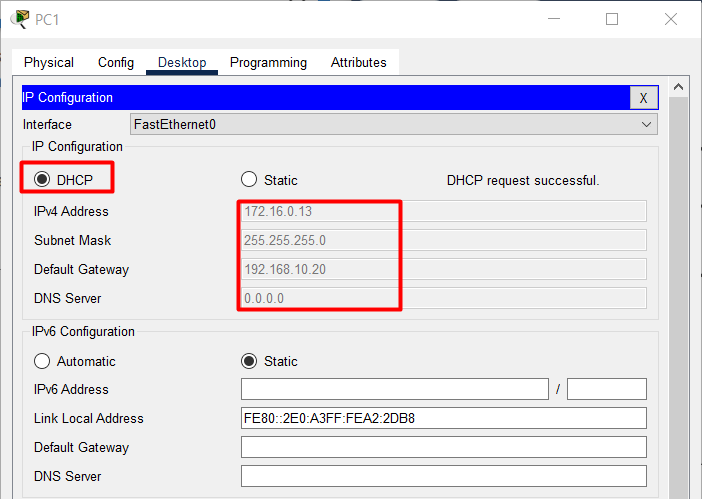
Kiểm thử

*Kịch bản 1: Switch1 chưa bật tính năng DAI*

Ở các PC tiến hành yêu cầu DHCP server



Hình 37: PC2 yêu cầu DHCP nhận IP thuộc lớp 192.168.0.0/24



Hình 38: PC2 yêu cầu DHCP nhận IP thuộc lớp 172.16.0.0/24

Nhận thấy rằng khi chưa bật tính năng DAI , các thiệt bị khi yêu cầu DHCP server thì có thể nhận được IP từ thuộc cả hai lớp 192.168.0.0/24 và 172.16.0.0/24 VLAN 1

*Kịch bản 2: Switch1 bật DAI và cho Fast Ethernet 0/8 về trust*

Cấu hình Switch1

Switch#config t

switch(config)# ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1 --> dùng vlan nào bật vlan đó

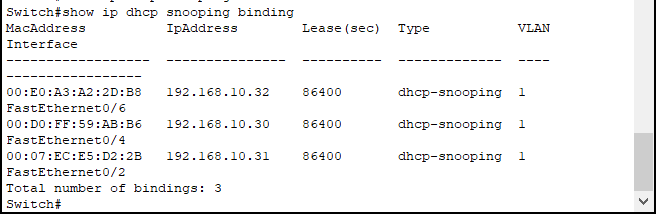
Switch(config)#no ip dhcp snooping information option --> loại bỏ trường 82 thêm vào

Switch(config)#int fa0/8 -- > Chỉ ra cổng trên switch muốn cấu hình

Switch(config-if)#ip dhcp snooping trust -- > Đặt về chế độ trust

Đứng từ các PC0, PC1, PC2 tiến hành yêu cầu DHCP , nhận thấy rằng các IP mà các PC này nhận được chỉ thuộc lớp mạng 192.168.0.0/24 VLAN 1

Cổng Fa0/10 (Kết nội giữa Switch1 và Server3) đã bị untrusted. Không thể cấp IP cho các PC.

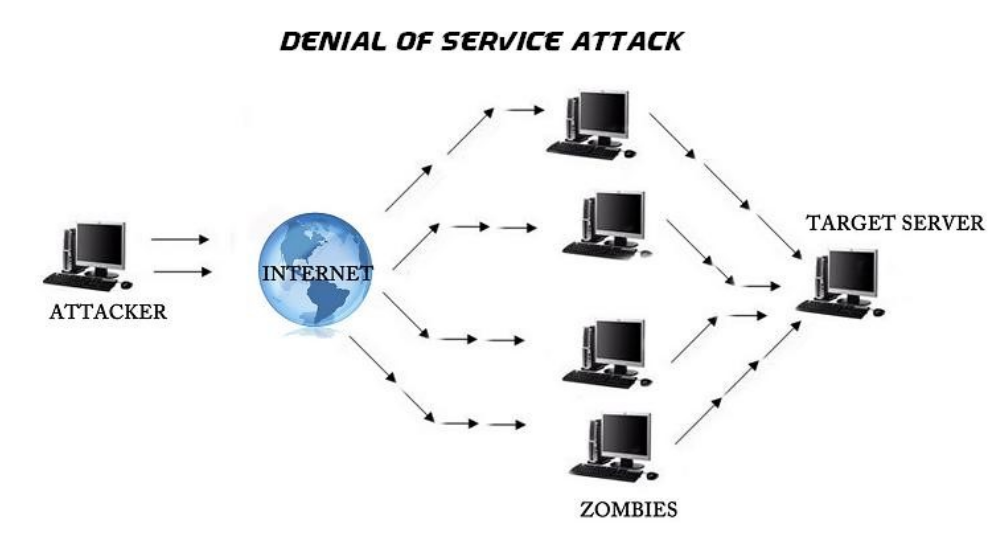


Hình 39: Xem nội dung bảng DHCP snooping bingding của Switch1

Bảng này sẽ lưu lại IP cũng như địa chỉ MAC của các thiết bị yêu cầu DHCP. Và nội dung của bảng này sẽ ko bị thay đổi. Mục đích của việc này là chống các cuộc tấn công ARP, attacker không thể thay đổi địa chỉ MAC thành địa chỉ nào khác chẳng hạn như chính địa chỉ MAC của attacker trong những cuộc tấn công ARP quy mô nhỏ. Bất kì các thiết bị nào yêu cầu DHCP với thông tin phân giải không đúng với nội dung đã lưu trong bảng DHCP snooping binding của Switch1 sẽ bị chặn lại.

**Tấn công DOS và DDOS**

**Mô hình tấn công**

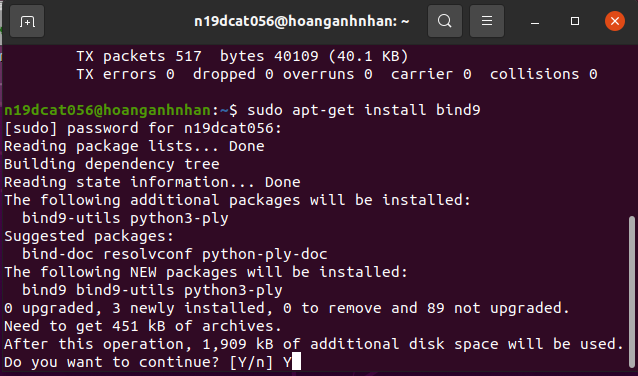
****

**Hình 40: Mô hình tấn công DDOS(https://www.digistar.vn/tan-cong-tu-choi-dich-vu-dos-va-ddos-phan-1/)**

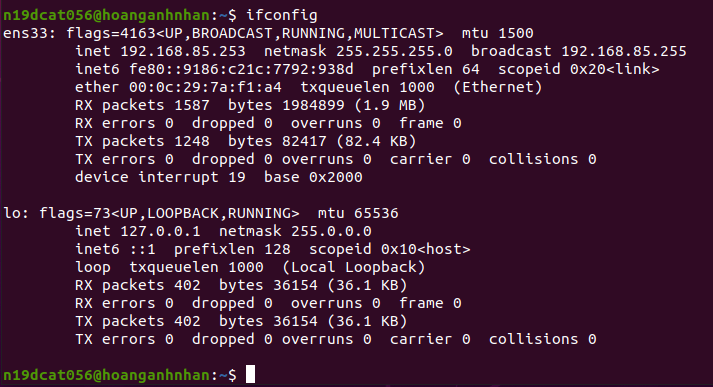
Tấn công

**2.1 Chuẩn bị và kiểm tra trước khi tấn công**

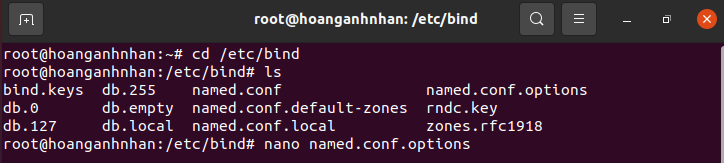
* **Cài đặt dns server cho máy nạn nhân**



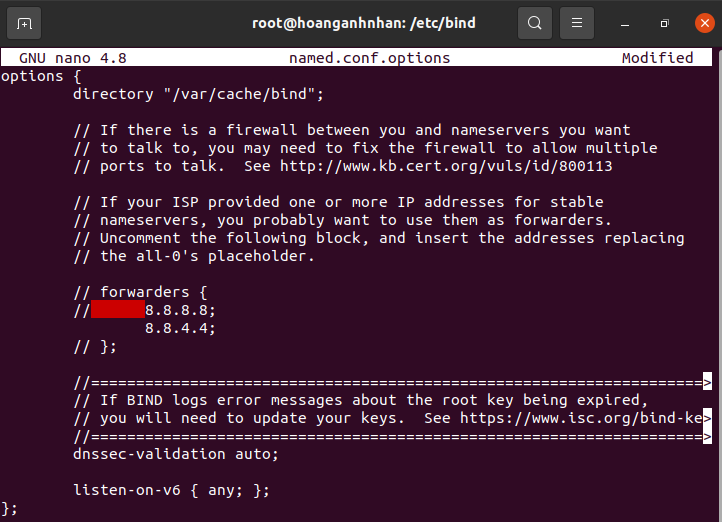
Hình 41: Cài đặt bind9 để thiết lập máy chủ DNS



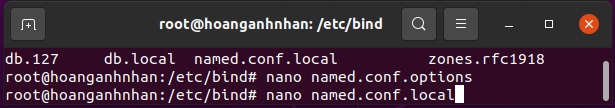
Hình 42: Kiểm tra IP của máy Ubuntu



Hình 43: Chỉnh sửa file cấu hình /etc/bind/named.conf.options



Hình 44: Chỉnh forwarders



Hình 45: Chỉnh sửa file cấu hình /etc/bind/named.conf.local



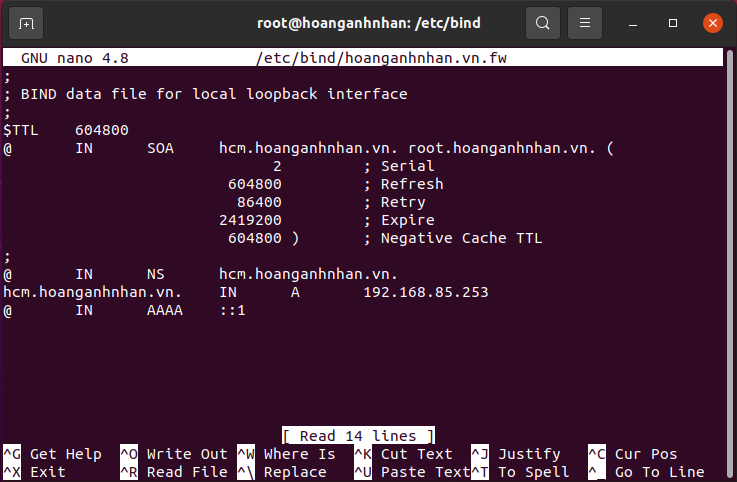
Hình 46: Thêm zone mới



Hình 47: Copy file /etc/bind/db.local qua /etc/bind/nhanhoanganh.vn.fw



Hình 48: Chỉnh sửa file /etc/bind/nhanhoanganh.vn.fw



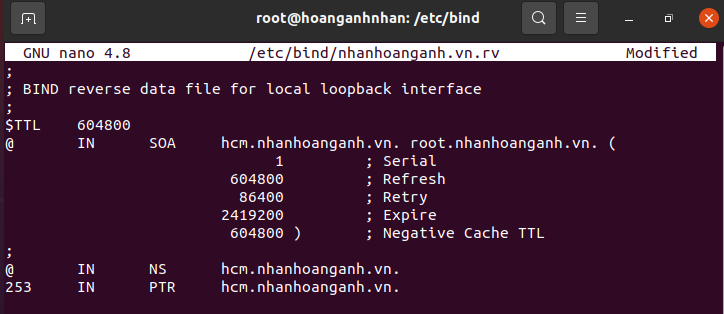
Hình 49: Cấu hình lại /etc/bind/nhanhoanganh.vn để nhận IP của DNS Server



Hình 50: Copy file /etc/bind/db.127 qua /etc/bind/nhanhoanganh.vn.rv



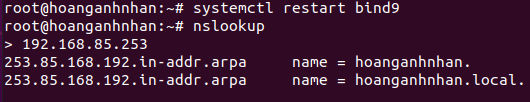
Hình 51: Chỉnh sửa file /etc/bind/db.10



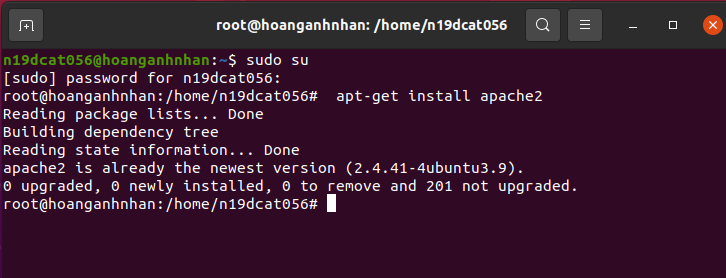
Hình 52: Cấu hình lại file /etc/bind/nhanhoanganh.vn.rv



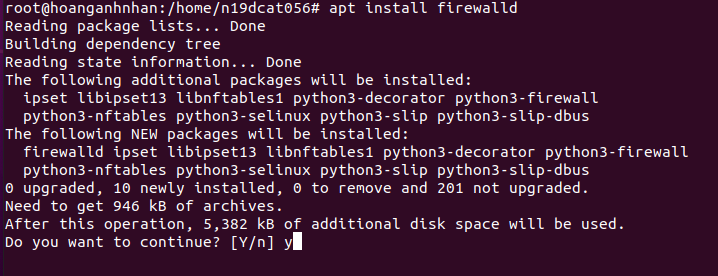
Hình 53 : Chỉnh sửa file /etc/resolv.conf



Hình 54 : Kết quả phân giải thành công



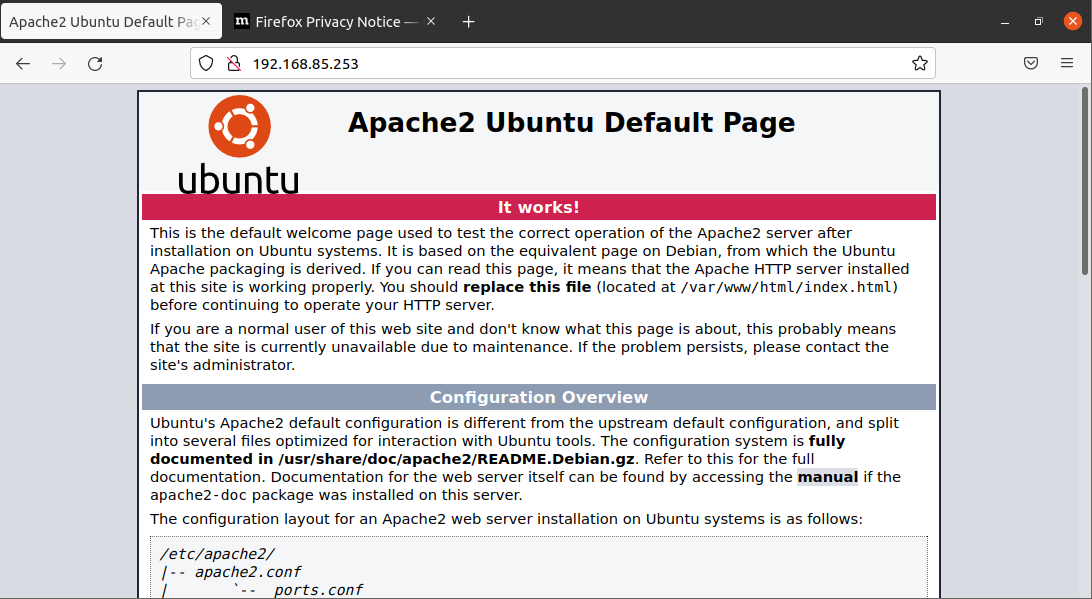
Hình 55: Cài đặt Apache cho máy Ubuntu dung làm DNS Server



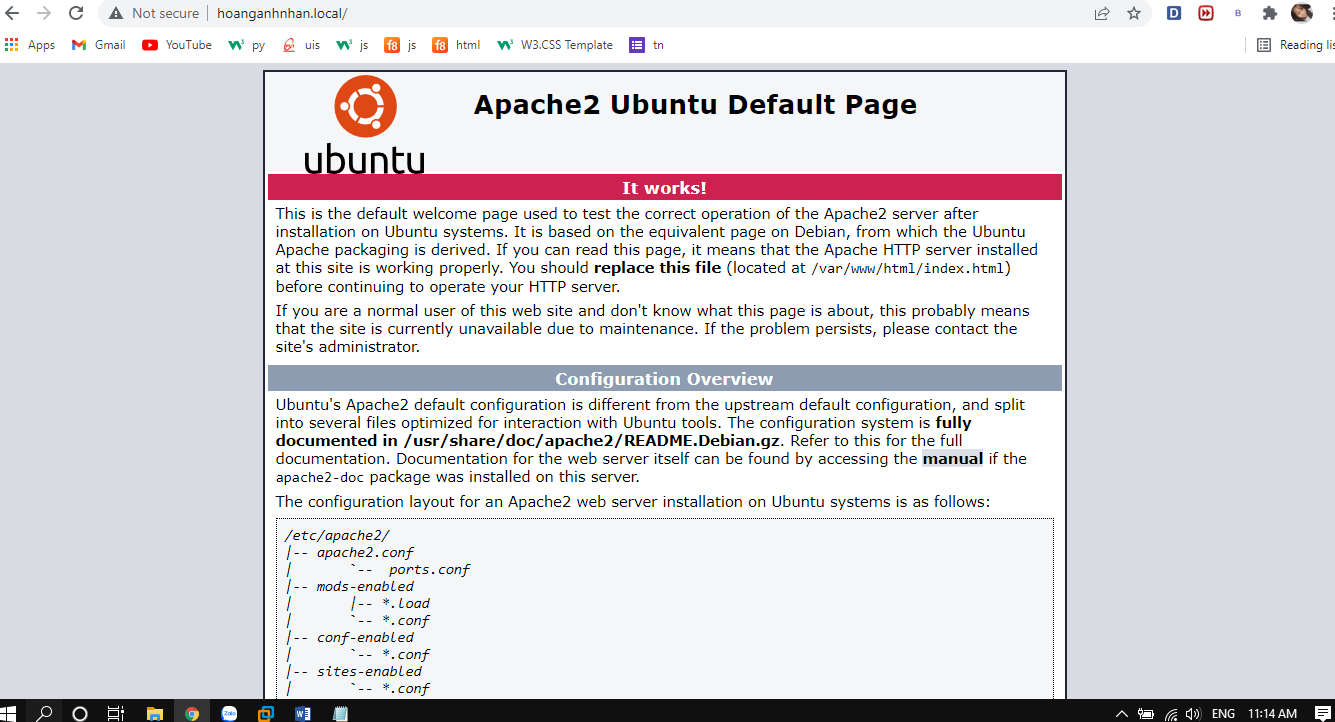
Hình 56: Cài đặt FirewallD



Hình 57: Mở port 80 và port 443 trên máy DNS Server để các máy khác trong mạng LAN có thể truy cập đến website của máy DNS Server

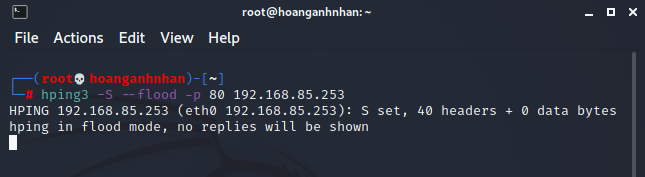


Hình 58: Cài đặt thành công có thể truy cập vào website mặc định của Apache trên DNS Server



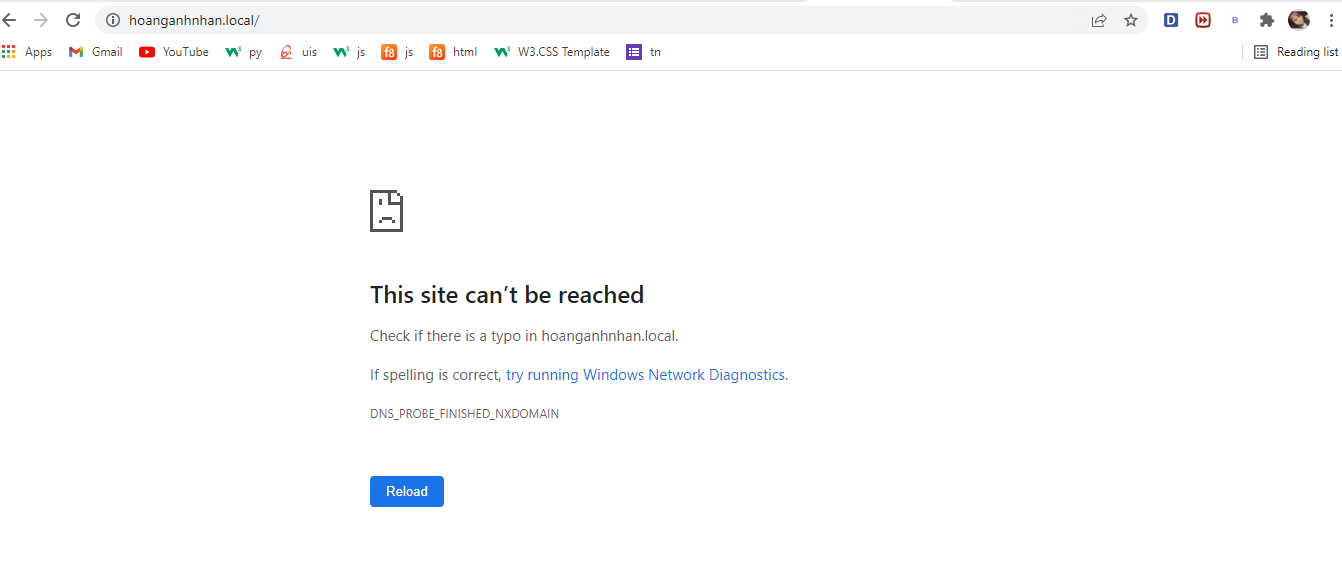
Hình 59: Máy thật mang IP 192.168.85.5 đã truy cập được website từ DNS Server

* 1. **Tấn công**



Hình 60: Máy Kali (Hacker) DDOS bằng flood

* 1. **Kết quả**



Hình 61: Máy Windows 10 đã không còn truy cập được vào website từ DNS Server

**Phòng thủ**

Có rất nhiều cách tấn công DDOS:

* Nếu bạn có thể xác định địa chỉ IP của các máy tính thực hiện tấn công: có thể tạo một danh sách quản lí truy cập trong tường lửa của bạn để chặn những IP này, thân chí chặn hoàn toàn IP từ các quốc gia nếu cần thiết
* Giám sát lưu lượng truy cập nhỏ, để nhanh chóng phát hiện tấn công DDOS nhỏ
* Mua thêm băng thông và thiết lập nhiều server

**KẾT LUẬN**

* Kết quả:
* Cấu hình thực hiện và hoàn thành đúng tiến độ và hiệu quả.
* Hạn chế:
* Do trong một thời gian ngắn nên nhóm cũng chưa thể tìm hiểu hết tất cả các

cơ chế bảo mật đối với dịch vụ DNS trên Kali Linux.

* Gặp một số hạn chế khi cấu hình trên Vmware do cấu hình máy yếu.
* Hướng phát triển:
* Nhóm sẽ tìm hiểu và tiếp tục cập nhật cấu hình phương thức tấn công cũng như bảo mật trong thời gian tới.

**Tài liệu tham khảo:**

<https://www.cloudflare.com/learning/dns/what-is-dns/>

<https://viblo.asia/p/tim-hieu-ve-co-che-load-balancing-GrLZD0X2Zk0#:~:text=Load%20Balancing%20l%C3%A0%20g%C3%AC%3F,d%E1%BB%A5ng%20c%E1%BB%A7a%20c%C3%A1c%20%E1%BB%A9ng%20d%E1%BB%A5ng>.

<https://vietnix.vn/arp-spoofing-la-gi/#:~:text=ARP%20spoofing%20c%C3%B2n%20%C4%91%C6%B0%E1%BB%A3c%20g%E1%BB%8Di,quy%E1%BB%81n%20truy%20c%E1%BA%ADp%20v%C3%A0o%20m%E1%BA%A1ng>.

<https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926>

TPHCM, ngày 13 tháng 03 năm 2022

**XÁC NHẬN CỦA GIẢNG VIÊN HƯỚNG DẪN**

ThS. Huỳnh Thanh Tâm TS.Huỳnh Trọng Thưa