

**BỘ CÔNG THƯƠNG**

**TRƯỜNG CAO ĐẲNG KỸ THUẬT CAO THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**…..** 🙦 🕮 🙤 **…..**



**ĐỒ ÁN MÔN HỌC**

***Đề tài***

**Tìm hiểu về Sniffing.**

**Giáo viên: Vũ Đức Toàn**

**Sinh viên thực hiện:**

**1. PHẠM PHÚC BẢO 0306201515**

**2. NGUYỄN THÀNH ĐỨC 0306201526**

**3. TRƯƠNG ANH NGUYÊN 0306201559**

**LỚP: CĐ TH 20MMTF Môn: An Ninh Mạng**

**KHÓA: 2020 – 2023**

**TP. HỒ CHÍ MINH, ngày 31 tháng 10 năm 2022**

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

**…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………...**

TP.HCM, Ngày …….Tháng…….Năm 2020

Giáo viên hướng dẫn

**MỤC LỤC**

[**1.** **Giới thiệu** 5](#_Toc118119549)

[1.1. Khái niệm Sniffing 5](#_Toc118119550)

[1.2. Cơ chế hoạt động của sniffing 6](#_Toc118119551)

[1.3. Phân loại Sniffing 6](#_Toc118119552)

[1.4. Các hình thức tấn công 7](#_Toc118119553)

[**2.** **Lắng nghe thông tin qua Hub** 7](#_Toc118119554)

[2.1. Phương pháp tấn công 7](#_Toc118119555)

[Hình 2.1.2: Xung đột khi nhiều thiết bị cùng truyền thông tại một thời điểm 8](#_Toc118119556)

[2.2. Các biện pháp phòng chống 8](#_Toc118119557)

[**3.** **Tấn công MAC** 9](#_Toc118119558)

[3.1. Khái niệm địa chỉ MAC 9](#_Toc118119559)

[3.2. Phương pháp tấn công 9](#_Toc118119560)

[3.3. Các biện pháp phòng chống 10](#_Toc118119561)

[**4.** **Tấn công DHCP** 10](#_Toc118119562)

[4.1. Khái niệm DHCP và quá trình cấp phát IP động 10](#_Toc118119563)

[4.2. DHCP Client giả 11](#_Toc118119564)

[4.3. DHCP Server giả 12](#_Toc118119565)

[4.4. Các biện pháp phòng chống 13](#_Toc118119566)

[**5.** **Chặn bắt thông tin dùng ARP - Poisoning** 13](#_Toc118119567)

[5.1. Khái niệm và nguyên tắc làm việc của ARP trong mạng LAN 13](#_Toc118119568)

[5.2. Cách thức hoạt động của ARP poisoning 14](#_Toc118119569)

[5.3. Các biện pháp phòng chống 16](#_Toc118119570)

[**6.** **Chặn bắt thông tin dùng DNS - Spoofing** 16](#_Toc118119571)

[6.1. Giao thức DNS 16](#_Toc118119572)

[6.2. Phương pháp tấn công DNS - Spoofing 16](#_Toc118119573)

[6.3. Các biện pháp phòng chống DNS - Spoofing 18](#_Toc118119574)

[**7.** **VLAN Hopping** 18](#_Toc118119575)

[7.1. Các giao thức hoạt động trong môi trường VLAN 18](#_Toc118119576)

[7.2. VLAN Hopping 20](#_Toc118119577)

[7.3. Các biện pháp phòng chống 21](#_Toc118119578)

[**8.** **Demo một số phương pháp tấn công Sniffing** 21](#_Toc118119579)

[8.1. Demo tấn công bằng WireShark: 21](#_Toc118119580)

[8.2. Quá trình thực hiện tấn công 21](#_Toc118119581)

**DANH MỤC HÌNH ẢNH**

[Hình 1.2.1: Cơ chế hoạt động của sniffing 6](#_Toc118119593)

[Hình 2.1.1: Lắng nghe thông tin qua Hub 8](#_Toc118119594)

[Hình 2.1.2: Xung đột khi nhiều thiết bị cùng truyền thông tại một thời điểm 9](#_Toc118119595)

[Hình 3.2.1: Kẻ tấn công đầu độc switch bằng địa chỉ MAC giả mạo 10](#_Toc118119596)

[Hình 3.2.2: Kẻ tấn công đã khiến switch hoạt động như một hub và 10](#_Toc118119597)

[Hình 4.1.1: Quá trình cấp phát IP từ máy chủ DHCP 12](#_Toc118119598)

[Hình 4.2.1: Attacker thực hiện “vét cạn” khiến dải địa chỉ IP có trên 13](#_Toc118119599)

[Hình 4.3.1: Hoạt động của DHCP Server giả mạo 13](#_Toc118119600)

[Hình 5.1.1: Cách thức hoạt động của ARP 15](#_Toc118119601)

[Hình 5.2.1: Chặn bắt thông tin dùng ARP Poisoning 16](#_Toc118119602)

[Hình 6.2.1: Mô hình tấn công DNS - Spoofing 18](#_Toc118119603)

[Hình 6.2.2: Tấn công giả mạo DNS sử dụng phương pháp ID Spoofing 18](#_Toc118119604)

[Hình 7.1.1: Giao thức VTP 20](#_Toc118119605)

[Hình 7.2.1: VLAN Hopping - Switch Spoofing 21](#_Toc118119606)

[Hình 7.2.2: Vlan Hopping - Double Tagging 22](#_Toc118119607)

[Hình 8.2.1: Thông tin máy tấn công 23](#_Toc118119608)

[Hình 8.2.2: Thông tin máy nạn nhân 24](#_Toc118119609)

[Hình 8.2.3: Thực hiện ping thông 2 máy 24](#_Toc118119610)

[Hình 8.2.4: Địa chỉ Default Gateway của máy tấn công và máy nạn nhân 25](#_Toc118119611)

[Hình 8.2.5: Lựa chọn card mạng phù hợp 25](#_Toc118119612)

[Hình 8.2.6: Giao diện chính của WireShark 26](#_Toc118119613)

[Hình 8.2.7: Phát hiện được địa chỉ IP của máy nạn nhân 26](#_Toc118119614)

[Hình 8.2.8: Đăng nhập techpanda.org với dạng giao thức http 27](#_Toc118119615)

[Hình 8.2.9: Máy tấn công thu thập những thông tin của máy nạn nhân 27](#_Toc118119616)

[Hình 8.2.10: Thông tin username và password đã bị lấy cắp 28](#_Toc118119617)

[Hình 8.2.11: Địa chỉ IP và MAC của máy nạn nhân đã bị thay đổi 28](#_Toc118119618)

[Hình 8.2.12: Địa chỉ MAC của hai máy trùng nhau 29](#_Toc118119619)

[Hình 8.2.13: Tắt các tính năng trên máy tấn công 29](#_Toc118119620)

[Hình 8.2.14: Địa chỉ MAC của máy nạn nhân trở về là địa chỉ ban đầu 30](#_Toc118119621)

**LỜI CẢM ƠN**

Tụi em xin gửi lời cảm ơn đến thầy Vũ Đức Toàn đã tận tình chỉ bảo và giúp đỡ nhóm em hoàn thành đồ án môn học này. Đồng thời qua đây, nhóm em xin gửi lời cảm ơn chân thành đến quý thầy cô Khoa Công nghệ Thông tin – Trường Cao đẳng Kỹ thuật Cao Thắng, những người đã trang bị cho chúng em những kiến thức để có thể giúp chúng em hoàn thành đồ án một cách tốt nhất.

Trong bài báo cáo, không thể không có sai sót. Kính mong nhận được ý kiến đóng góp của quý thầy cô để bài báo cáo của nhóm em hoàn thiện tốt hơn.

Em xin chân thành cảm ơn..

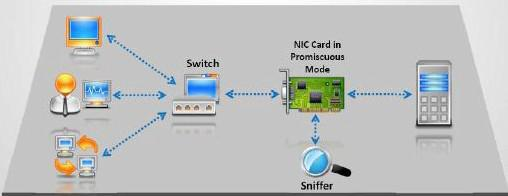
# **Giới thiệu**

## Khái niệm Sniffing

Sniffing là một hình thức nghe lén trên hệ thống mạng dựa trên những đặc điểm của cơ chế TCP/IP. Người nghe lén để thiết bị lắng nghe giữa mạng mang thông tin như hai thiết bị điện thoại hoặc hai thiết bị đầu cuối trên internet. Nghe lén được sử dụng như công cụ để các nhà quản trị mạng theo dõi, bảo trì hệ thống mạng và có thể kiểm tra các dữ liệu ra vào mạng. Về mặt tiêu cực, nó được sử dụng với mục đích nghe lén các thông tin trên mạng để lấy các thông tin quan trọng.

## Cơ chế hoạt động của sniffing

Những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân. Bởi vậy để hiểu được những dữ liệu này, các chương trình nghe lén phải có tính năng phân tích các nghi thức, cũng như tính năng giải mã các dữ liệu ở dạng nhị phân để hiểu được chúng.



Hình 1.2.1: Cơ chế hoạt động của sniffing

**Trong môi trường Hub:** Một khung gói tin khi chuyển từ máy A sang máy B thì đồng thời nó gửi đến tất cả các máy khác đang kết nối cùng Hub theo cơ chế loan tin (broadcast). Các máy khác nhận được gói tin này sẽ tiến hành so sánh yêu cầu về địa chỉ MAC của frame gói tin với địa chỉ đích. Nếu trùng lập thì sẽ nhận, còn không thì cho qua. Do gói tin từ A được gửi đến B nên khi so sánh thì chỉ có B mới giống địa chỉ đích đến nên chỉ có B mới thực hiện tiếp nhận.

Dựa theo nguyên tắc đó, máy được cài đặt chường trình nghe trộm sẽ “tự nhận” bất cứ gói tin được lưu chuyển trong mạng qua Hub, kể cả khi đích đến gói tin có đích đến không phải là nó, do sniffer chuyển card mạng của máy sang chế độ hỗn tạp (promiscuous mode). Promiscuous mode là chế độ đặc biệt. Khi card mạng được đặt dưới chế độ này, nó có thể nhận tất cả các gói tin mà không bị ràng buộc kiểm tra địa chỉ đích đến.

**Trong môi trường Switch:**Khác với Hub, Switch chỉ chuyển tải các gói tin đến những địa chỉ cổng xác định trong bảng chuyển mạch nên nghe trộm kiểu “tự nhận” như Hub không thực hiện được. Tuy nhiên, kẻ tấn công có thể dùng các cơ chế khác để tấn công trong môi trường Switch như ARP spoofing, MAC spoofing, MAC duplicating, DNS spoofing, v.v…

## Phân loại Sniffing

* Passive sniffing: Chủ yếu họat động trong môi trường không có các thiết bị chuyển mạch gói, phổ biến hiện nay là các dạng mạng sử dụng Hub. Do không có các thiết bị chuyển mạch gói nên các gói tin được broadcast đi trong mạng. Chính vì vậy, việc thực hiện sniffing là khá đơn giản. Kẻ tấn công không cần gửi ra gói tin giả mạo nào, chỉ cần bắt các gói tin từ Port về (dù host nhận gói tin không phải là nơi đến của gói tin đó). Hình thức sniffing này rất khó phát hiện do các máy tự broadcast các gói tin. Ngày nay hình thức này thường ít được sử dụng do Hub không còn được ưa chuộng nhiều, thay vào đó là Switch.
* Active sniffing:Chủ yếu hoạt động trong môi trường có các thiết bị chuyển mạch gói, phổ biến hiện nay là các dạng mạch sử dụng Switch. Kẻ tấn công thực hiện sniffing dựa trên cơ chế ARP và RARP (2 cơ chế chuyển đổi từ IP sang MAC và từ MAC sang IP) bằng cách phát đi các gói tin đầu độc, mà cụ thể đây là phát đi các gói thông báo cho máy gửi gói tin là “tôi là người nhận” mặc không phải là “người nhận”.Ngoài ra, các sniffer còn có thể dùng phương pháp giả địa chỉ MAC, thay đổi MAC của bản thân thành MAC của một máy hợp lệ và qua được chức năng lọc MAC của thiết bị, qua đó ép dòng dữ liệu đi qua card mạng của mình. Tuy nhiên, do gói tin phải gửi đi nên sẽ chiếm băng thông. Nếu thực hiện sniffing quá nhiều máy trong mạng thì lượng gói tin gửi đi sẽ rất lớn (do liên tục gửi đi các gói tin giả mạo) có thể dẫn đến nghẽn mạng.

## Các hình thức tấn công

Sniffing là hình thức nghe lén thông tin trên mạng nhằm khai thác hiệu quả hơn tài nguyên mạng, theo dõi thông tin bất hợp pháp. Tuy nhiên, sau này các hacker dùng sniffing để lấy các thông tin nhạy cảm, do đó cũng có thể coi đó là 1 hình thức hack. Có khá nhiều các phương pháp để thực hiện sniffing, dù là tấn công chủ động hay bị động. Sau đây là 6 phương pháp tấn công sniffing:

1) Lắng nghe thông tin qua Hub

2) Tấn công MAC

3) Tấn công DHCP

4) Chặn bắt thông tin dùng ARP – poisoning

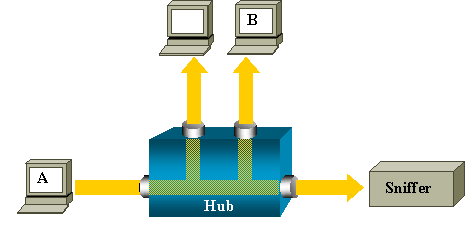
5) Chặn bắt thông tin dùng DNS – spoofing

6) VLAN Hopping

# **Lắng nghe thông tin qua Hub**

## Phương pháp tấn công

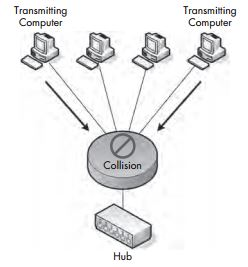
Sniffing trên mạng môi trường Hub là 1 giấc mơ đối với bất kỳ ai, bửi gói tin được gửi đi qua thiết bị Hub thì sẽ đi qua tất cả các cổng kết nối với Hub đó. Một khung gói tin khi chuyển từ máy A sang máy B thì đồng thời nó gửi đến tất cả các máy khác đang kết nối cùng Hub theo cơ chế loan tin (broadcast).



Hình 2.1.1: Lắng nghe thông tin qua Hub

Để phân tích lưu lượng đi qua 1 máy tính kết nối với 1 thiết bị Hub thì chỉ cần kết nối một packet sniffer tới 1 cổng còn trống trên Hub. Tuy nhiên, những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân. Vì thế các chương trình nghe lén phải có chức năng giải mã dữ liệu ở dạng nhị phân để hiểu được chúng. Ngoài ra, kẻ tấn công sẽ chuyển card mạng sang chế độ Promiscuous. Chế độ Promiscuous cho phép card mạng nhìn thấy tất cả các gói tin đi qua hệ thống dây mạng. Khi card mạng được đặt dưới chế độ này, nó có thể nhận tất cả các gói tin mà không bị ràng buộc kiểm tra địa chỉ đích đến. Từ đó, kẻ tấn công có thể thấy được tất cả truyền thông đến và đi từ máy tính đó, cũng như truyền thông giữa các thiết bị khác kết nối với thiết bị Hub.

Tuy nhiên, ngày nay mạng Hub không còn được ưa chuộng bởi vì chỉ có 1 thiết bị duy nhất có thể truyền thông tại một thời điểm, 1 thiết bị kết nối qua 1 Hub phải cạnh tranh băng thông với các thiết bị khác cũng đang cố gắng truyền thông qua thiết bị Hub đó. Khi hai hay nhiều thiết bị truyền thông ngay tại cùng một thời điểm, sẽ dễ xảy ra xung đột.



Hình 2.1.2: Xung đột khi nhiều thiết bị cùng truyền thông tại một thời điểm

Kết quả gây ra sẽ là mất mát gói tin, và các thiết bị sẽ phải truyền lại các gói tin đó, khiến cho mạng càng trở nên tắc nghẽn. Khi đến 1 mức xung đột nào đó, thiết bị sẽ phải truyền lại một gói tin đến tận 3,4 lần và sẽ làm giảm hiệu năng của mạng. Ngoài ra, hình thức tấn công qua Hub rất khó bị phát hiện do các máy tự broadcast các gói tin. Vì thế nên dù Hub có tiện lợi, dễ sử dụng nhưng ngày nay, hầu hết các mạng đều sử dụng Switch thay cho Hub.

## Các biện pháp phòng chống

Phương pháp lắng nghe thông tin qua Hub khó phát hiện và phòng chống, vì kẻ tấn công chỉ tiến hành lắng nghe trên đường truyền và bắt giữ lại những gói tin mà không có sự tác động đáng kể nào vào hệ thống. Vì thế một trong những cách đơn giản nhất là làm cách nào để các gói tin không còn broadcast nữa, bằng cách sử dụng Switch thay cho Hub. Ngoài ra có thể dùng phương pháp “lấy độc trị độc” là sử dụng chính các công cụ nghe lén để phát hiện mình có bị nghe lén hay không. Các công cụ này ngoài việc thực hiện tác vụ nghe lén, còn có khả năng dò tìm trên mạng nội bộ có máy nào đang nghe lén hay không.

# **Tấn công MAC**

## Khái niệm địa chỉ MAC

Địa chỉ MAC (Media Access Control) là kiểu địa chỉ vật lí, đặc trưng cho một thiết bị hoặc một nhóm các thiết bị trong LAN. Địa chỉ này được dùng để nhận diện các thiết bị giúp cho các gói tin lớp 2 có thể đến đúng đích.

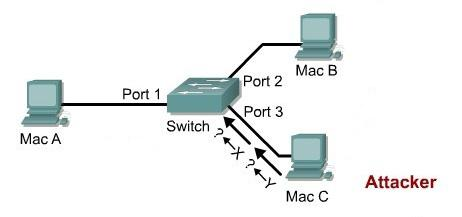
Địa chỉ MAC gồm một bộ sáu cặp hai ký tự, cách nhau bằng dấu hai chấm. Ví dụ 00:1B:44:11:3A:B7 là một địa chỉ MAC.

## Phương pháp tấn công

Tấn công MAC là kỹ thuật khá phổ biến trong mạng LAN. Mục đích của kỹ thuật này là làm ngập lụt switch với một số lượng lớn yêu cầu. Thoạt nhìn thì thấy đây chỉ là mục đích phá hoại nhưng đối tượng tấn công có thể đi xa hơn khi tận dụng để nghe lén các gói tin của người khác.

Kẻ tấn công phải nằm trong chính mạng LAN đó và sử dụng một ứng dụng phần mềm để tạo thật nhiều frame với địa chỉ MAC giả mạo (MAC spoofing) rồi gửi đến switch. Khi nhận được frame này, switch không phân biệt được đâu là giả đâu là thật và sẽ xem nó như một frame bình thường. Lúc này, switch sẽ cập nhật các địa chỉ MAC mới vào bảng CAM.

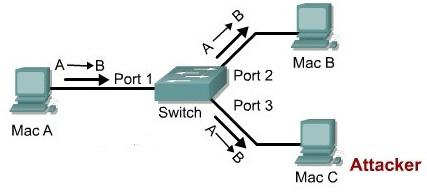
Bảng CAM (Content Addressable Memory), cũng có thể gọi là bảng MAC, là nơi lưu trữ các địa chỉ MAC của các port và các tham số VLAN trong switch. Nhờ vào bảng CAM, switch có thể biết được một thiết bị có địa chỉ MAC X đang nằm ở port vật lý nào để còn đẩy frame trả lời về port đó. Kẻ tấn công sẽ đầu độc switch liên tục toàn các địa chỉ MAC giả mạo. Bảng CAM của switch thì có kích thước giới hạn, nên đến một thời điểm nào đó bảng CAM sẽ bị đầy.



Hình 3.2.1: Kẻ tấn công đầu độc switch bằng địa chỉ MAC giả mạo

khiến bản CAM bị đầy

Khi máy A gửi gói tin đến máy B, nó sẽ tìm trong bảng địa chỉ MAC của nó, coi thử có địa chỉ MAC của máy B hay không, nếu không có máy A sẽ gửi gói tin ARP request đến switch để hỏi địa chỉ MAC của máy B. Máy B lúc này nhận được gói tin sẽ gửi phản hồi lại cho máy A sau đó các gói tin được lưu chuyển từ A đến B mà không chuyển sang các máy khác. Tuy nhiên, lúc này bảng CAM đã bị đầy tràn, các lưu lượng ARP request sẽ làm ngập lụt mỗi cổng của switch. Switch đã bị lụt với các gói tin của các địa chỉ MAC khác nhau và sẽ broadcast lưu lượng mà không cần thông qua bảng CAM nữa. Đến lúc này thì switch hoạt động không khác gì hub. Kẻ tấn công sẽ sử dụng 1 công cụ Packet Sniffer để thâu tóm các dữ liệu mong muốn.



Hình 3.2.2: Kẻ tấn công đã khiến switch hoạt động như một hub và

lắng nghe thông tin trong mạng

## Các biện pháp phòng chống

Nguyên lí chung của các phương pháp phòng chống là không để các gói tin có địa chỉ MAC lạ đi qua switch. Phương pháp phòng chống hiệu quả nhất là cấu hình port security trên switch. Đây là một đặc trưng cấu hình cho phép điều khiển việc truy cập vào cổng switch thông qua địa chỉ MAC của thiết bị gắn vào. Khi switch nhận được một gói tin chuyển đến, nó sẽ kiểm tra địa chỉ MAC nguồn của gói tin với danh sách các địa chỉ đã được cấu hình trước đó. Nếu hai địa chỉ này khác nhau thì tuỳ theo sự cấu hình của người quản trị mà switch sẽ xử lí gói tin đến với các mức độ khác nhau.

Các lệnh cấu hình port security:

- Switch(config-if)# switchport mode access 19

- Switch(config-if)# switchport port-security: cho phép cổng được hoạt động trong chế độ port-security.

- Mặc định thì cổng chỉ cho phép một địa chỉ MAC (một thiết bị) được

gán vào và số địa chỉ có thể nằm trong khoảng từ 1 đến 1024.

- Switch(config-if)# sw port-security violation shutdown: Nếu vi phạm sẽ tắt cổng, kẻ tấn công sẽ không thể làm tràn bảng CAM.

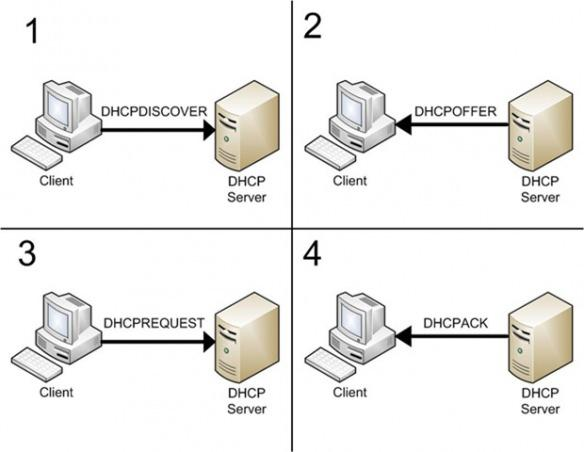
# **Tấn công DHCP**

## Khái niệm DHCP và quá trình cấp phát IP động

DHCP (Dynamic Host Configuration Protocol - giao thức cấu hình host động) là một giao thức cho phép cấp phát địa chỉ IP một cách tự động cùng với các cấu hình liên quan khác như subnet mark và gateway mặc định.

Quá trình truyền thông giữa một máy tính trạm được cấu hình sử dụng IP động (DHCP Client) với một máy đảm nhận chức năng cấp phát IP động (DHCP Server) diễn ra như sau:

* Đầu tiên, một DHCP Client muốn nhận mới một địa chỉ IP lên toàn mạng (broadcast) một thông điệp **“**DHCP Discover” có chứa địa chỉ MAC của nó để tìm kiếm sự hiện diện của DHCP server. 
* Sau đó, nếu có DHCP Server thuộc cùng subnet với DHCP Client trên server này sẽ phản hồi lại cho client bằng một thông điệp **“**DHCP Offer” có chứa một địa chỉ IP như là một lời đề nghị cho “thuê” (lease) địa chỉ.
* Tiếp theo, khi nhận được gói “DHCP Offer” đến đầu tiên, client sẽ trả lời lại cho server một thông điệp **“**DHCP Request” như là sự chấp thuận lại đề nghị.
* Cuối cùng, server gửi lại cho client thông điệp **“**DHCP Acknowledgment” để xác nhận lần cuối với client. Và từ đây client có thể sử dụng địa chỉ IP vừa “thuê” được để truyền thông với các máy khác trên mạng.

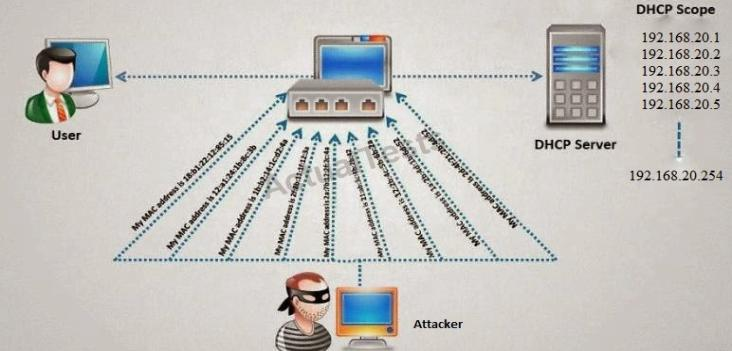


Hình 4.1.1: Quá trình cấp phát IP từ máy chủ DHCP

Tuy có nhiều ưu điểm, nhưng giao thức DHCP lại hoạt động khá đơn giản, suốt quá trình trao đổi thông điệp giữa DHCP Server và DHCP Client không có sự xác thực hay kiểm soát truy cập nên dễ phát sinh một số điểm yếu về an toàn. DHCP Server không thể biết được rằng mình đang liên lạc với một DHCP Client bất hợp pháp hay không, ngược lại DHCP Client cũng không thể biết DHCP Server đang liên lạc có hợp pháp không. Trong mạng có khả năng xuất hiện các DHCP Client giả và DHCP Server giả.

## DHCP Client giả

Trong trường hợp này, DHCP Client là một máy trạm bất hợp pháp. Attacker có thể thoả hiệp thành công với một client hợp pháp nào đó trong mạng, sau đó thực hiện các chương trình cài đặt. Các chương trình thực thi trên client này thực hiện “vét cạn”, liên tục gửi tới DHCP Server các gói tin yêu cầu xin cấp IP với các địa chỉ MAC không có thực, cho tới khi dải IP có sẵn trên DHCP Server cạn kiệt vì bị thuê hết. Điều này dẫn tới việc DHCP Server không còn địa chỉ IP nào để cho các DHCP Client hợp pháp thuê, khiến dịch vụ bị ngưng trệ , các máy trạm khác không thể truy nhập vào hệ thống mạng để truyền thông với các máy tính trong mạng.

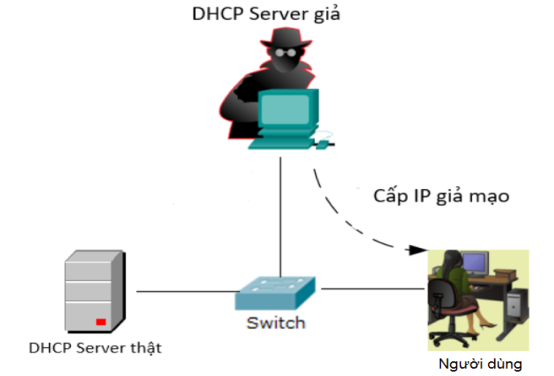


Hình 4.2.1: Attacker thực hiện “vét cạn” khiến dải địa chỉ IP có trên

DHCP Server bị cạn kiệt

## DHCP Server giả

Kẻ tấn công sẽ tạo ra một server giả mạo vào trong mạng. Server này có khả năng phản hồi DHCP discovery request t phía client. Vậy nên cả server giả mạo và server thực đều có khả năng phản hồi các yêu cầu của client và server nào đáp ứng trước sẽ kiểm soát được client đó. DHCP server giả mạo có thể gán địa chỉ IP của mình thành default gateway cho client. Như vậy, tất cả các thông tin từ client sẽ được gửi tới địa chỉ của kẻ tấn công. Kẻ tấn công sau khi thu thập tất cả những thông tin này, rồi chuyển đến default gateway đúng của mạng. Vì thế client vẫn truyền bình thường với các máy ngoài mạng mà không hề biết họ đã để lộ thông tin cho kẻ tấn công. Loại tấn công này rất khó bị phát hiện bởi client trong một thời gian dài.



Hình .: Hoạt động của DHCP Server giả mạo

Nguy hiểm hơn, nếu kẻ tấn công phá vỡ được các hàng rào bảo vệ mạng và đoạt được quyền kiểm soát DHCP Server thì có thể tạo ra những thay đổi trong cấu hình của DHCP Server theo ý muốn. Khi đó, kẻ tấn công có thể thiết lập lại dải IP, subnet mask,… của hệ thống để các máy trạm hợp pháp không thể đăng nhập vào hệ thống mạng được, tạo ra tình trạng từ chối dịch vụ trong mạng hay làm những việc gây ảnh hưởng xấu đến toàn hệ thống mạng.

## Các biện pháp phòng chống

Kẻ tấn công đã dùng phương pháp “vét cạn”, liên tục gửi tới DHCP Server các gói tin yêu cầu xin cấp IP với các địa chỉ MAC không có thực, cho tới khi dải IP có sẵn trên DHCP Server cạn kiệt vì bị thuê hết. Vì thế cần phải có biện pháp ngăn chặn việc này như:

- Xây dựng một bảng chứa thông tin liên quan giữa: địa chỉ MAC máy client - địa chỉ IP - VLAN - số hiệu cổng. Bảng này dùng để giám sát việc xin cấp phát địa chỉ IP của các máy client, tránh việc 1 máy client xin cấp phát nhiều địa chỉ IP.

- Quy định số lượng gói tin DHCP đến 1 cổng/đơn vị thời gian. Ngoài ra có thể sử dụng một số giải pháp của các hãng công nghệ.

* Hãng Cisco đã đưa công nghệ DHCP snooping (giám sát DHCP) vào thiết bị switch. Ý tưởng chính của công nghệ này là:

- Cấu hình các cổng trên switch thành 2 kiểu: cổng trust và cổng untrust.

- Cổng trust là cổng có thể cho phép gửi đi tất cả các loại các bản tin, được nối với máy chủ DHCP.

- Cổng untrust là cổng chỉ có thể gửi đi bản tin xin cấp phát địa chỉ IP.

Cổng untrust thường là cổng nối với các thiết bị đầu cuối người dùng. Do vậy máy tính của kẻ tấn công mặc dù là một máy chủ DHCP, nhưng không thể gửi các bản tin DHCP cấp phát địa chỉ IP giả mạo.

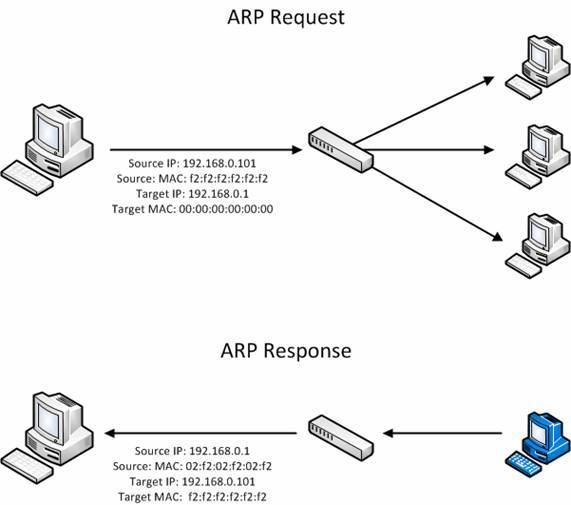
# **Chặn bắt thông tin dùng ARP - Poisoning**

## Khái niệm và nguyên tắc làm việc của ARP trong mạng LAN

Tầng Network của mô hình OSI sử dụng các loại địa chỉ mang tính chất quy ước như IP, IPX… Trên thực tế, các card mạng (NIC) chỉ có thể kết nối với nhau theo địa chỉ MAC, địa chỉ cố định và duy nhất của phần cứng. Chính vì vậy, giao thức phân giải địa chỉ: Address Resolution Protocol (ARP) được sử dụng để chuyển đổi các dạng địa chỉ này qua lại với nhau.

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ tầng network (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại một ARP reply cho thiết bị gửi ARP request (trong đó có chứa địa chỉ MAC của mình).

Lấy ví dụ trong một hệ thống mạng đơn giản, khi PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP request broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của PC có địa chỉ IP này là gì?". Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy đó là địa chỉ IP của mình, PC B sẽ gửi lại một gói tin ARP reply cho PC A, trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.



Hình 5.1.1: Cách thức hoạt động của ARP

ARP là một giao thức phi trạng thái. Máy chủ mạng sẽ tự động lưu trữ bất kỳ ARP reply nào mà chúng nhận được, bất kể máy khác có yêu cầu hay không. Ngay cả các mục ARP chưa hết hạn sẽ bị ghi đè khi nhận được gói tin ARP reply mới. Không có phương pháp nào trong giao thức ARP mà giúp một máy có thể xác nhận máy mà từ đó gói tin bắt nguồn. Hành vi này là lỗ hổng cho phép ARP spoofing xảy ra.

## Cách thức hoạt động của ARP poisoning

Giao thức ARP vốn được thiết kế ra nhằm mục đích tạo tính thuận tiện để trao đổi địa chỉ giữa lớp thứ 2 và lớp thứ 3 của mô hình OSI. Lớp thứ hai, hay còn gọi với cái tên khác là tầng data-link, sử dụng địa chỉ MAC để các thiết bị phần cứng có thể giao tiếp với nhau một cách trực tiếp trong một diện nhỏ. Còn với lớp thứ 3, tên khác là tầng network, thì lại sử dụng địa chỉ IP để tạo ra một mạng với diện rộng hơn để có thể giao tiếp trên toàn cầu.

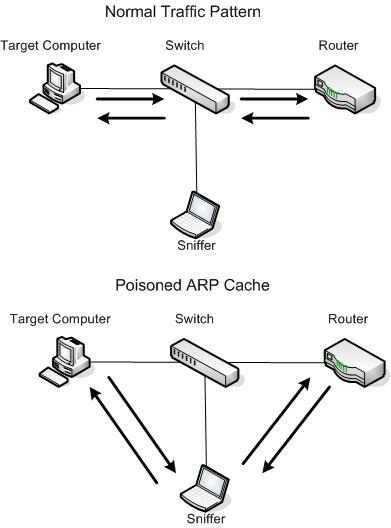
Tổ chức của giao thức ARP vốn xoay quanh hai gói tin chính, đó là ARP

request và ARP reply. Mục đích chính của gói tin request và reply là để định vị được địa chỉ MAC của thiết bị phần cứng tương ứng với địa chỉ IP mà nó được gán cho. Từ đó, các luồng dữ liệu mới có thể được truyền đi tới đích trong một mạng mà không bị thất lạc hay nhầm lẫn máy tính khác không yêu cầu gói tin đó.

Để hiểu được tính chất request và reply, ta hình dung đơn giản như sau. Gói request sẽ được gửi đi cho từng thiết bị trong mạng và phát đi thông điệp “Xin chào, địa chỉ IP của tôi là X.X.X.X, và địa chỉ MAC của tôi là X:X:X:X:X:X. Tôi cần gửi một thứ đến một máy có địa chỉ IP là Y.Y.Y.Y, nhưng tiếc thay tôi không có địa chỉ MAC của anh ấy. Vậy ai có địa chỉ IP như tôi vừa nói thì vui lòng phản hồi kèm theo địa chỉ MAC của anh để tôi trao gói tin này.”

Lúc này, máy cần phản hồi sẽ đưa ra gói ARP reply với thông điệp “Tôi là người anh cần tìm đây. Tôi có địa chỉ IP là Y.Y.Y.Y và MAC của tôi là Y:Y:Y:Y:Y:Y”. Khi quá trình truyền giao gói tin hoàn tất, thiết bị phát sẽ cập nhật bảng ARP cache của nó và hai thiết bị này có thể truyền thông với nhau.

Việc đầu độc gói tin ARP này chính là đánh vào yếu tố bất lợi và không bảo mật của giao thức ARP ban đầu. Rõ ràng qua đoạn trên cũng có thể thấy được tính bất cập của gói ARP request và reply. Bất kỳ một máy tính nào đó không phải mang địa chỉ Y.Y.Y.Y nhưng hắn cũng có thể lấn quyền máy thật và giả mạo rằng mình mang IP đó, và sau đó đem địa chỉ MAC của mình ra cung cấp. Bên request không có cơ chế kiểm soát chặt chẽ người đứng ra nhận, mà chỉ căn cứ vào mỗi địa chỉ IP rồi chấp nhận chuyển đi.



Hình 5.2.1: Chặn bắt thông tin dùng ARP Poisoning

Đặc biệt, giao thức ARP không giống như DNS chỉ có thể được cấu hình để chấp nhận các nâng cấp động (dynamic updates), các thiết bị sử dụng giao thức ARP sẽ chấp nhận cập nhật bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào có thể gửi gói ARP reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP cache của nó ngay giá trị mới này. Việc gửi một gói ARP reply khi không có request nào được tạo ra gọi là việc gửi ARP “cho không”. Khi các ARP reply cho không này đến được các máy tính đã gửi request, máy tính request này sẽ nghĩ rằng đó chính là người mình đang tìm kiếm để truyền tin, tuy nhiên thực chất họ lại đang bắt đầu thiết lập kết nối với một kẻ xấu giả danh để thực hiện cho việc tấn công MITM.

## Các biện pháp phòng chống

Ngày nay với sự phát triển của các phần mềm bảo mật cũng như sự ra đời của giao thức HTTPS, ARP - Poisoning đã không còn hiệu quả như lúc trước. Có thể kể đến một vài biện pháp để phòng chống như:

* Bảo mật LAN

Giả mạo ARP Cache là một kỹ thuật tấn công mà nó chỉ sống sót khi cố gắng chặn lưu lượng giữa hai thiết bị trên cùng một LAN. Chỉ có một lý do đáng lo ngại về vấn đề này là liệu thiết bị nội bộ trên mạng có bị thỏa hiệp, hoặc ai đó có thể cắm một thiết bị không tin cậy vào mạng. Mặc dù tập trung toàn bộ những cố gắng bảo mật của mình lên phạm vi mạng nhưng việc phòng chống lại những mối đe dọa ngay từ bên trong và việc có một thái độ bảo mật bên trong tốt có thể giúp ta loại trừ được loại tấn công này.

* Mã hóa ARP Cache

Một cách có thể bảo vệ chống lại vấn đề không an toàn vốn có trong các ARP request và ARP reply là thực hiện một quá trình kém động hơn. Đây là một tùy chọn vì các máy tính Windows cho phép ta bổ sung các entry tĩnh vào ARP cache. Trong các trường hợp, nơi cấu hình mạng không mấy khi thay đổi, ta hoàn toàn có thể tạo một danh sách các entry ARP tĩnh và sử dụng chúng cho các client thông qua một kịch bản tự động. Điều này sẽ bảo đảm được các thiết bị sẽ luôn dựa vào ARP cache nội bộ của chúng thay vì các ARP request và ARP reply.

* Kiểm tra lưu lượng ARP với chương trình của hãng thứ ba

Tùy chọn cuối cùng cho việc phòng chống lại hiện tượng giả mạo ARP cache là phương pháp phản ứng có liên quan đến việc kiểm tra lưu lượng mạng của các thiết bị. Ta có thể thực hiện điều này với một vài hệ thống phát hiện xâm phạm (chẳng hạn như Snort) hoặc thông qua các tiện ích được thiết kế đặc biệt cho mục đích này (như xARP). Điều này có thể khả thi khi ta chỉ quan tâm đến một thiết bị nào đó, tuy nhiên nó vẫn khá cồng kềnh và vướng mắt trong việc giải quyết với toàn bộ đoạn mạng.

# **Chặn bắt thông tin dùng DNS - Spoofing**

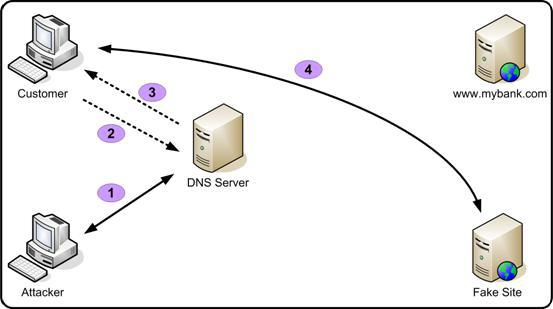
## Giao thức DNS

Giao thức DNS (Domain Name System – hệ thống phân giải tên miền) là một giao thức quan trọng nhất được dùng trong Internet, cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Mỗi website có một tên (là tên miền hay đường dẫn URL) và một địa chỉ IP. 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).

## Phương pháp tấn công DNS - Spoofing

DNS – spoofing là một kĩ thuật cung cấp thông tin DNS sai lệch cho

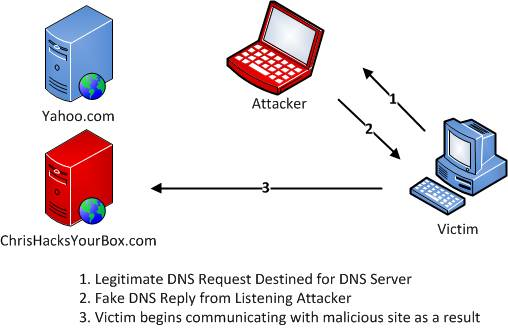
một host. Khi người dùng yêu cầu truy cập đến một địa chỉ website thì nó sẽ chuyển hướng, đưa người dùng tới một địa chỉ giả mạo có hình thức giống với địa chỉ thật và họ không hề hay biết rằng mình đang bị lừa. Kẻ tấn công sẽ lấy cắp được những thông tin nhạy cảm của người dùng, hoặc cài các phần mềm độc hại, hay có thể gây ra một từ chối dịch vụ nào đó.



Hình 6.2.1: Mô hình tấn công DNS - Spoofing

Một ví dụ , khi người dùng cần truy cập hộp thư điện tử của mình tại địa chỉ www.mybank.com có địa chỉ IP là X.X.X.X thì khi đó, kỹ thuật này sẽ chuyển hướng yêu cầu sang một trang giả mạo có địa chỉ IP là Y.Y.Y.Y do kẻ tấn công dựng nên để chiếm đoạt tài khoản của người dùng.

Có nhiều phương pháp triển khai kỹ thuật DNS Spoofing, đơn giản nhất là DNS ID Spoofing. Mỗi truy vấn DNS được gửi đi qua mạng đều có chứa một số nhận dạng duy nhất. Mục đích của số nhận dạng là phân biệt các truy vấn và phản hồi chúng một cách chính xác. Để chặn một truy vấn DNS nào đó được gửi đi từ máy nạn nhân, kẻ tấn công sẽ tạo một gói giả mạo có chứa số nhận dạng đó để gói dữ liệu được chấp nhận bới máy nạn nhân.



Hình 6.2.2: Tấn công giả mạo DNS sử dụng phương pháp ID Spoofing

Quá trình tấn công này được thực hiện với hai bước. Đầu tiên, tiến hành ARP Cache Poisoning thiết bị, mục đích là để định tuyến lại lưu lượng của nó qua host đang sử dụng để tấn công của mình, từ đó có thể chặn yêu cầu DNS và gửi đi gói dữ liệu giả mạo để lừa nạn nhân truy cập vào website giả mạo của kẻ tấn công dựng nên thay vì vào thẳng website chính thức mà họ đang cố gắng truy cập.

## Các biện pháp phòng chống DNS - Spoofing

Tấn công DNS Spoofing rất khó để phòng chống vì có khá ít các dấu hiệu tấn công. Nạn nhân sẽ không thể nhận ra là mình đang bị chuyển hướng truy cập vào trang giả mạo cho đến khi thấy có gì đó bất thường khi tiến hành đăng nhập. Hoặc nếu kẻ tấn công không khéo léo, thì nạn nhân mới nhận ra có điều gì đó khác thường ngay lúc giao diện trang web hiện ra.

* Một số hướng phòng chống tấn công DNS Spoofing:
* Bảo mật hệ thống máy tính của bạn: Các dạng tấn công này thường xuất phát ngay từ trong nội bộ. Nếu làm công tác bảo mật tốt ngay từ yếu tố môi trường thật, yếu tố con người thì việc bị lợi dụng để chuyển hướng DNS là điều bất khả thi.
* Tránh sử dụng DNS cho các hệ thống bảo mật: Điều này đồng nghĩa, nếu môi trường đó có chứa dữ liệu nhạy cảm của công ty, thì việc hạn chế sử dụng Internet, cấm truy cập mạng các máy tính đó là điều cần thiết.
* Sử dụng IDS: Một dạng hệ thống phát hiện dấu hiệu xâm nhập. Khi được đặt và triển khai trên hệ thống cửa ta, nó có thể phát hiện các hình thức giả mạo ARP cache và giả mạo DNS.
* Sử dụng DNSSEC: DNSSEC là một giải pháp thay thế mới cho DNS, sử dụng các bản ghi DNS có chữ ký (Signature) để bảo đảm sự hợp lệ hóa của đáp trả truy vấn. Giải pháp này đã có sự triển khai nhất định.

# **VLAN Hopping**

## Các giao thức hoạt động trong môi trường VLAN

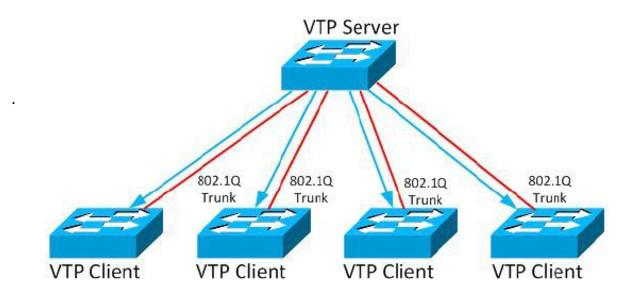
* Các chuẩn đóng gói VLAN

Khi sử dụng nhiều VLAN trong mạng có các Switch được nối với nhau, giữa các Switch sẽ được kết nối trunk. Đường trunk này có nhiệm vụ truyền frame của các VLAN khác nhau cùng một lúc. Khi gửi frame tới một Switch khác, các Switch cần một cách để định ra các VLAN mà frame muốn gửi tới. Vì thế chúng ta cần một chuẩn để đóng gói các frame để các switch phân biệt được frame đó của VLAN nào.

* Inter-switch link (ISL): Đây là chuẩn độc quyền của cisco nên chỉ có thể sử dụng trên các switch của cisco. ISL đóng gói toàn bộ các frame Ethernet gốc trong một ISL header. Các frame Ethernet được đóng gói bên trong không có gì thay đổi. Trong ISL header sẽ gán vlan ID, dựa vào vlan ID này nên Switch nhận biết được frame thuộc VLAN nào gửi tới.
* IEEE 802.1Q: Đây là một chuẩn dùng chung cho tất cả các thiết bị. Chuẩn này được sử dụng cho môi trường mạng LAN, 802.1Q sử dụng hoàn toàn khác với ISL, nó không đóng gói frame gốc mà nó thêm vào header của frame 4 bytes. Trong 4 bytes đó thì sẽ chứa VLAN ID và dựa vào VLAN ID mà switch có thể nhận biết ra frame thuộc VLAN nào.
* Giao thức VLAN Trunking Protocol (VTP)

VTP là giao thức độc quyền của Cisco hoạt động ở lớp 2 của mô hình OSI. VTP giúp cho việc cấu hình VLAN luôn đồng nhất khi thêm, xóa, sửa thông tin về VLAN trong một hệ thống mạng. VTP được thiết lạp để giải quyết các vấn đề nằm bên trong hoạt động của môi trường mạng VLAN.

Ví dụ: Một hệ thống có các kết nối Switch hỗ trợ bởi các VLAN. Để thiết lập và duy trì kết nối bên trong VLAN, mỗi VLAN phải được cấu hình thông suốt trên tất cả các Switch. Khi phát triển mạng và các Switch được thêm vào mạng, mỗi Switch mới phải được cấu hình với các thông tin của VLAN trước đó. Lúc này với VTP cho phép chỉ cần tạo VLAN trên server thông tin sẽ được phân phối đến các switch khác, nếu có thay đổi VLAN thì giữa các Switch sẽ tự động đồng bộ với nhau. VTP sử dụng các gói tin VTP Advertisement để đồng bộ. Theo chu kỳ 5 phút 1 lần các Switch sẽ gửi gói tin này cho các Switch nối trực tiếp với nó. Mặc định thì VTP đã được bật trên Switch nhưng không tắt giao thức này được.



Hình 7.1.1: Giao thức VTP

Để thực hiện đồng bộ thông tin của cấu hình VLAN thì phải thỏa mãn 2 điều kiện sau:

* Có đường trunk nối các switch lại với nhau.
* Các Switch phải cùng chung 1 miền VTP

VTP chỉ giúp đồng bộ thông tin cấu hình VLAN chứ không đồng bộ cổng. Vì vậy phải cấu hình gán cổng cho các VLAN trên Switch.

* Giao thức Dynamic Trunking Protocol (DTP)

DTP là giao thức độc quyền của cisco dùng để thiết lập đường trunk và cách đóng gói frame VLAN (chuẩn IEEE 802.1Q hoặc chuẩn ISL) giữa 2 Switch. Có thể cấu hình đường trunk bằng tay giữa hai thiết bị chuyển mạch. Nhưng với giao thức DTP thì đường trunk được thiết lập một cách tự động. Theo mặc định thì giao thức DTP đã được bật trên các thiết bị chuyển mạch của Cisco. Giữa Router và Switch có thể cấu hình đường trunk nhưng không có giao thức này vì Router không hiểu được giao thức DTP. Người quản trị mạng có thể cấu hình trạng thái DTP trên mỗi trunk port. Các trạng thái bao gồm: on, off, desirable, auto và non- negotiate.

* On: Trạng thái này được sử dụng khi Switch khác không hiểu giao thức DTP.
* Off: Trạng thái này được sử dụng khi cổng đã được cấu hình từ trước không với mục đích trở thành trunk port.
* Desirable: Trạng thái này được sử dụng khi cổng Switch muốn trở thành trunk port.
* Auto: Đây là trạng thái mặc định trên nhiều Switch.
* Non- negotiate: trạng thái này được sử dụng khi người quản trị muốn một loại trunk được đóng gói ISL hay IEEE 802.1Q cụ thể.

Trên phần lớn Switch giao thức DTP trên các cổng được cấu hình mặc định là auto.

## VLAN Hopping

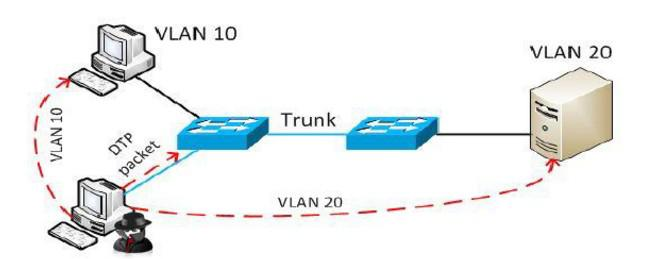
VLAN Hopping là một phương thức tấn công mạng dựa trên những yếu tố của VLAN. Attacker sử dụng VLAN Hopping khi muốn đi vòng qua các thiết bị lớp 2, lớp 3 khi trao đổi thông tin từ một VLAN này sang một VLAN khác. Ý tưởng tấn công dựa trên các trunk port trên Switch được cấu hình bất hợp lý. Mặc định, các trunk port có thể truy cập tới tất cả các VLAN.Dữ liệu truyền qua các đường trunk này có thể được đóng gói theo chuẩn IEEE 802.1Q hoặc ISL (Inter – Switch Link).

VLAN Hopping có thể được sử dụng để ăn cắp mật khẩu và các thông tin nhạy cảm khác từ các thuê bao mạng cụ thể. VLAN hopping cũng có thể được sử dụng để sửa đổi, làm hỏng, hoặc xóa dữ liệu, hay cài đặt phần mềm gián điệp hoặc các chương trình phần mềm độc hại khác và lan truyền virus, worms, Trojan trong mạng.

VLAN Hopping được thực hiện theo 2 cách: Switch Spoofing và Double Tagging.

* VLAN Hopping với Switch Spoofing:

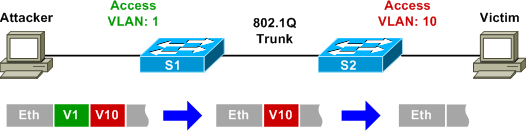
Tất cả các trunk port đều có thể truy cập tới tất cả các VLAN. Nếu Attacker kết nối vào trunk port thì Attacker sẽ thấy được tất cả các gói tin của tất cả các VLAN bằng các phần mềm Sniffer. Để tiến hành tấn công VLAN Hopping theo kiểu Switch Spoofing, Attacker sẽ gửi các gói tin được đóng gói theo các chuẩn Inter- Switch Link (ISL) hoặc 802.1Q cùng với Dynamic Trunking Protocol (DTP), để thiết lập kết nối trunk đến Switch. Theo mặc định thì trạng thái DTP trên mỗi trunk port trên Switch đều ở chế độ auto, khi Attacker gửi DTP packet đến Switch thì Switch sẽ kết nối trunk với Attacker. Do đó, Attacker sẽ dễ dàng truy cập vào tất cả các VLAN. Attacker có thể gửi packet hoặc nhận các packet tới bất kỳ VLAN nào.



Hình 7.2.1: VLAN Hopping - Switch Spoofing

* VLAN Hopping với Double Tangging:

Kiểu tấn công này lợi dụng cách thức hoạt động của Switch. Hiện nay, phần lớn các Switch chỉ thực hiện đóng gói IEEE 802.1Q. Điều này cho phép Attacker trong những tình huống cụ thể có khả năng gắn các đuôi 802.1Q (gọi là .1Q tag) vào khung. Khung này sẽ vào VLAN với đuôi .1Q đầu ra không xác định. Một đặc điểm quan tr ng của kiểu tấn công VLAN Hopping Double Tagging là nó thậm chí có thể tiến hành với các cổng trunk đã được thiết lập ở chế độ off.



Hình 7.2.2: Vlan Hopping - Double Tagging

## Các biện pháp phòng chống

* Cách phòng chống tấn công VLAN Hopping với Switch Spoofing: tắt tính năng trunking trên tất cả các port ngoài trừ port dùng để kết nối đến các Switch khác. Trên port trunk thì cũng tắt tính năng Dynamic trunking (DTP), chỉ cấu hình trunk tĩnh.
* Cách phòng chống tấn công VLAN Hopping với Double Tagging: Kiểu tấn công này chỉ xảy ra khi native VLAN trên đường trunk trùng với VLAN mà Attacker sử dụng để tấn công. Vì thế cần cài đặt native trên các đường trunk là một VLAN không có user nào sử dụng (không có port nào gán vào VLAN này - unused VLAN).

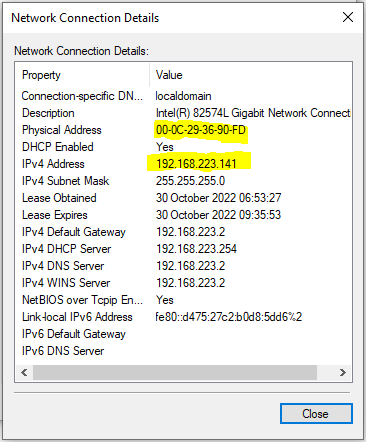
# **Demo một số phương pháp tấn công Sniffing**

## Demo tấn công bằng WireShark:

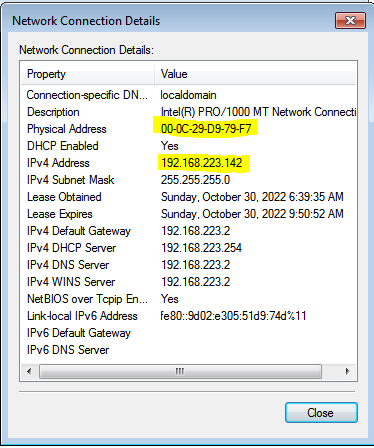
* Công cụ thực hiện demo:
* Một máy tính chạy hệ điều hành Windows 7 đóng vai trò máy nạn nhân, có:
* Địa chỉ IP: 192.168.223.142
* Địa chỉ MAC: 00-0C-29-D9-79-F7
* Một máy tính chạy hệ điều hành Windows 10 đóng vai trò máy tấn công, có:
* Địa chỉ IP: 192.168.223.141
* Địa chỉ MAC: 00-0C-29-36-90-FD
* Công cụ hỗ trợ tấn công WireShark.

## Quá trình thực hiện tấn công

Kiểm tra địa chỉ IP và MAC của máy tấn công và máy nạn nhân

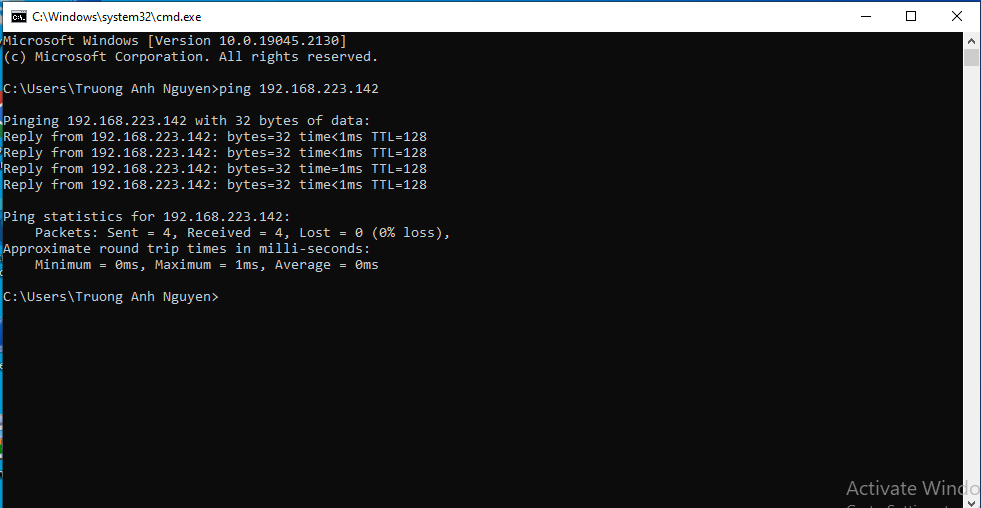


Hình 8.2.1: Thông tin máy tấn công



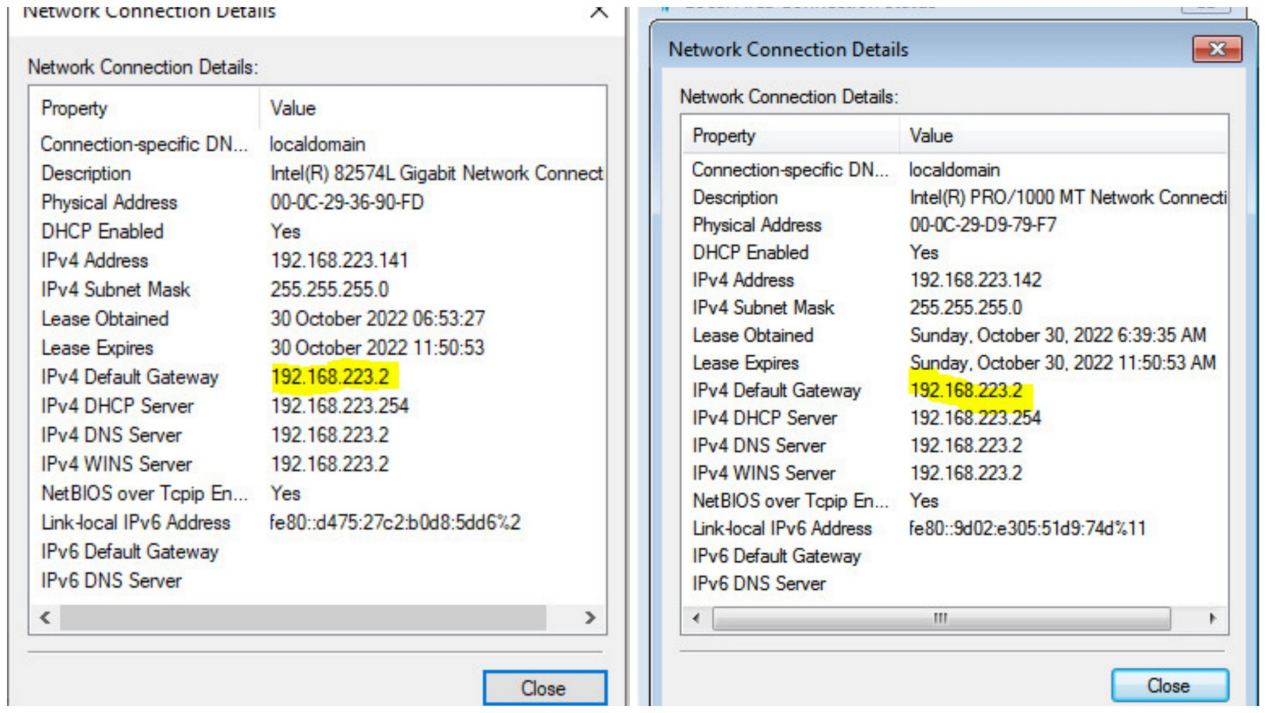
Hình 8.2.2: Thông tin máy nạn nhân

Sau khi kiểm tra thông tin của hai máy, quay về máy tấn công và tiến hành ping hai máy để chúng hoạt động trên cùng một mạng LAN. Ở máy tấn công, gõ lệnh ip và địa chỉ IP của máy nạn nhân.



Hình 8.2.3: Thực hiện ping thông 2 máy

Sau khi ping thông thành công, 2 máy sẽ có cùng địa chỉ Default Gateway

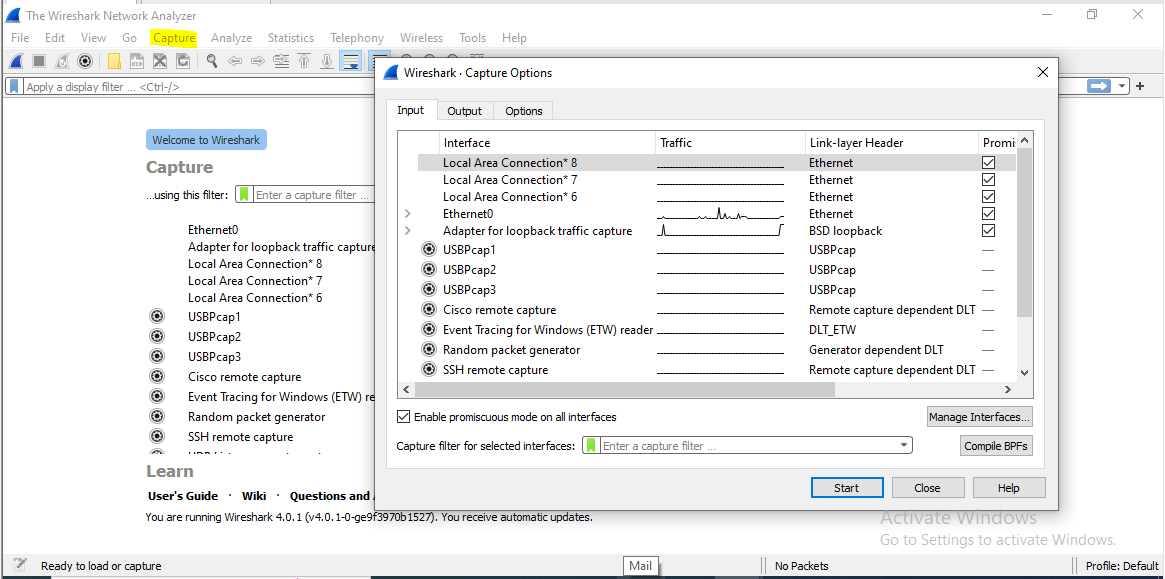


Hình 8.2.4: Địa chỉ Default Gateway của máy tấn công và máy nạn nhân

* Thực hiện trên máy tấn công

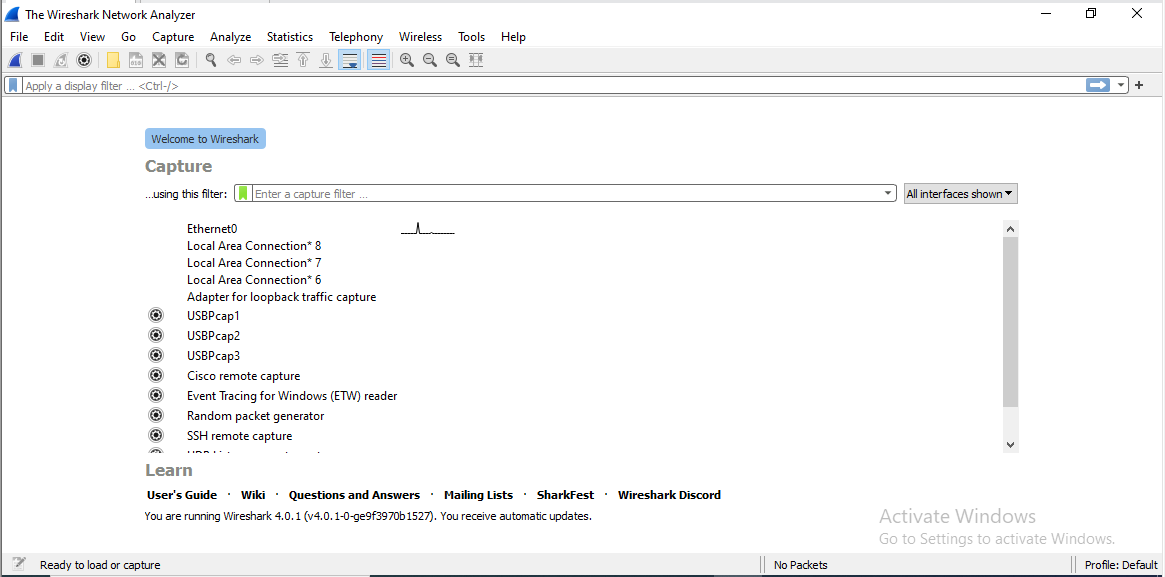
Tiếp theo, máy tấn công sẽ mở bộ công cụ hỗ trợ tấn công WireShark để thực hiện tấn công.

Trước hết, vào mục Capture chọn Options để chọn card mạng phù hợp, và sau đó nhấn Start để tiến hành nghe lén.



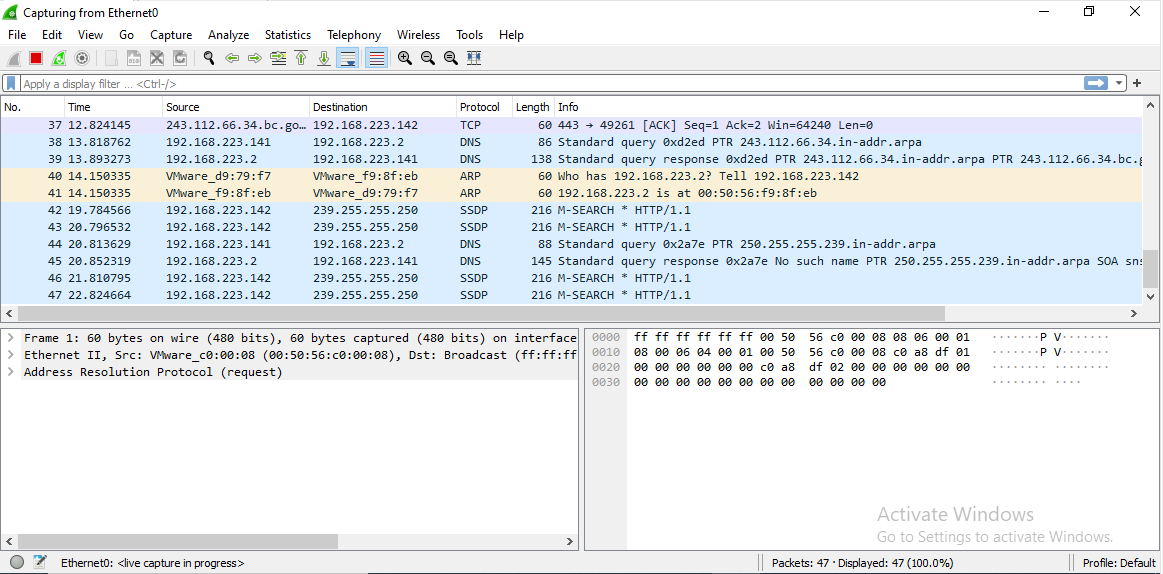
Hình 8.2.5: Lựa chọn card mạng phù hợp

Hoặc ta cũng có thể chọn ngay trên giao diện chính của WireShark bằng cách nháy đúp vào card mạng muốn chọn.



Hình 8.2.6: Giao diện chính của WireShark

Sau khi Start, địa chỉ IP của máy nạn nhân đã hiện lên.

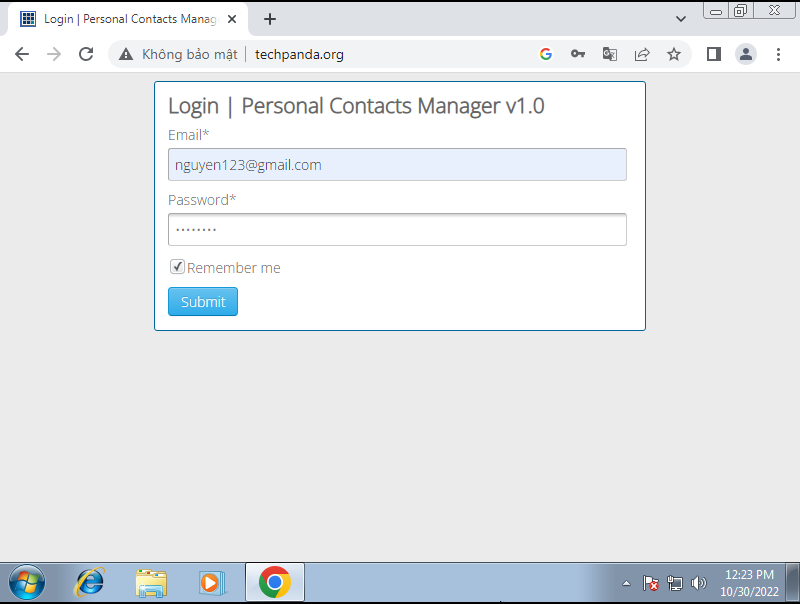


Hình 8.2.7: Phát hiện được địa chỉ IP của máy nạn nhân

* Thực hiện trên máy nạn nhân

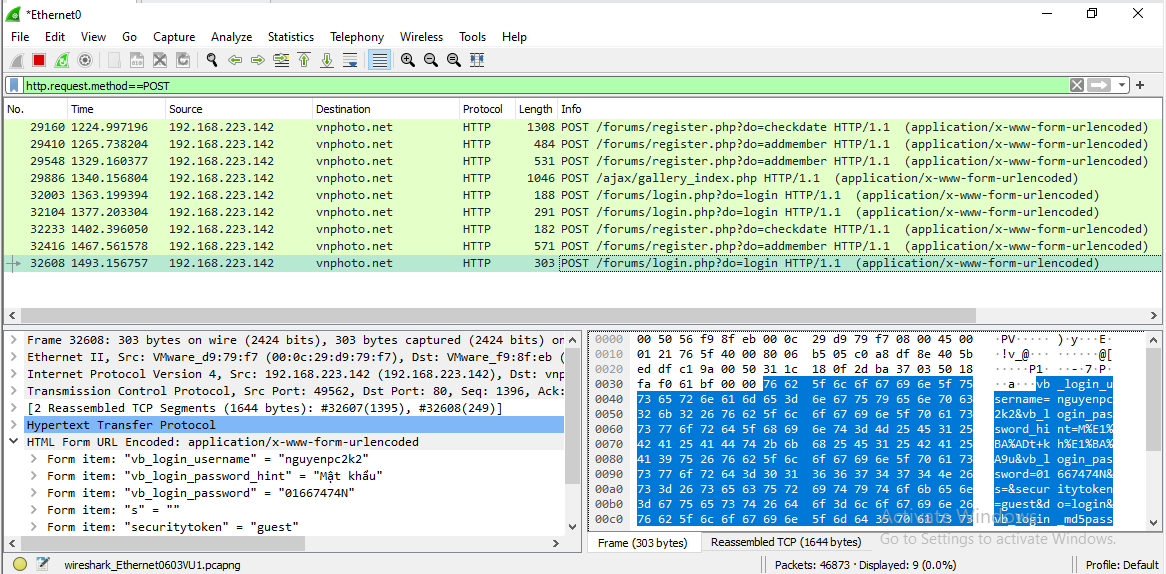
Chuyển sang máy nạn nhân, mở một trình duyệt bất kì và truy cập vào một trang web

* Lưu ý: phải là trang web http vì nó không có mã hóa, nếu nó là https thì chúng ta sẽ không nhìn thấy được username và password vì nó đã mã hóa.



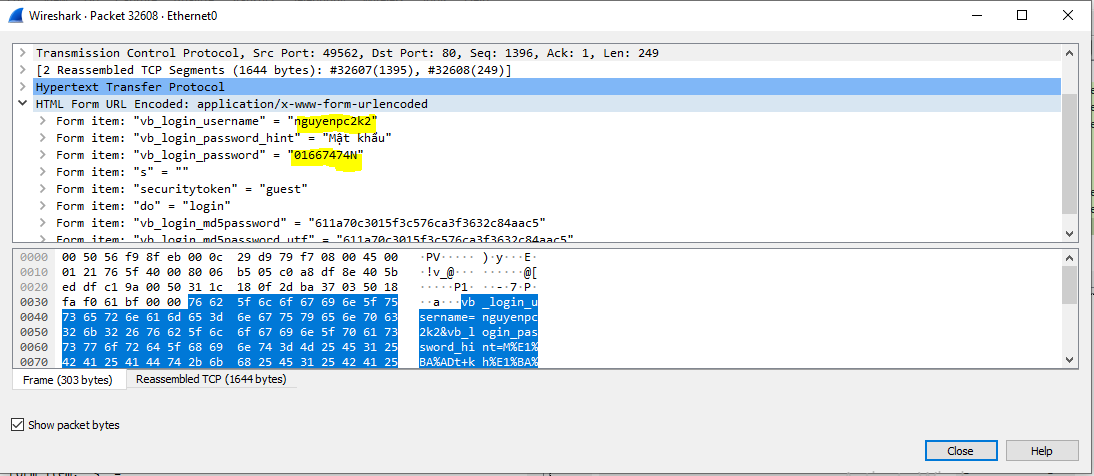
Hình 8.2.8: Đăng nhập techpanda.org với dạng giao thức http

Sau đó chuyển về máy của kẻ tấn công, mở công cụ WireShark nhấn vào thanh Apply a display filter .... (hoặc nhấn Ctrl + /) gõ “http.request.method==POST”



Hình 8.2.9: Máy tấn công thu thập những thông tin của máy nạn nhân

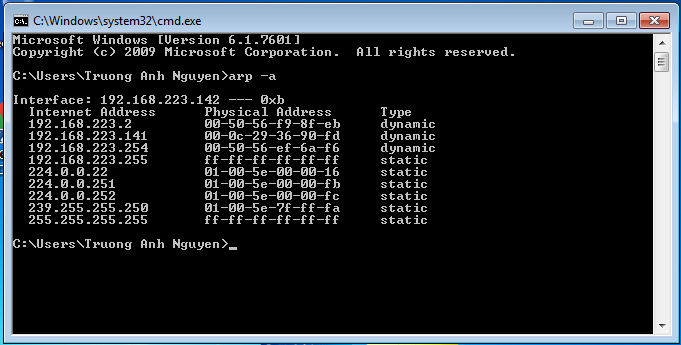
Lúc này máy tấn công đã thu thập được Username và Password, ta chỉ cần nháy đúp vào gói tin để xem kết quả.



Hình 8.2.10: Thông tin username và password đã bị lấy cắp

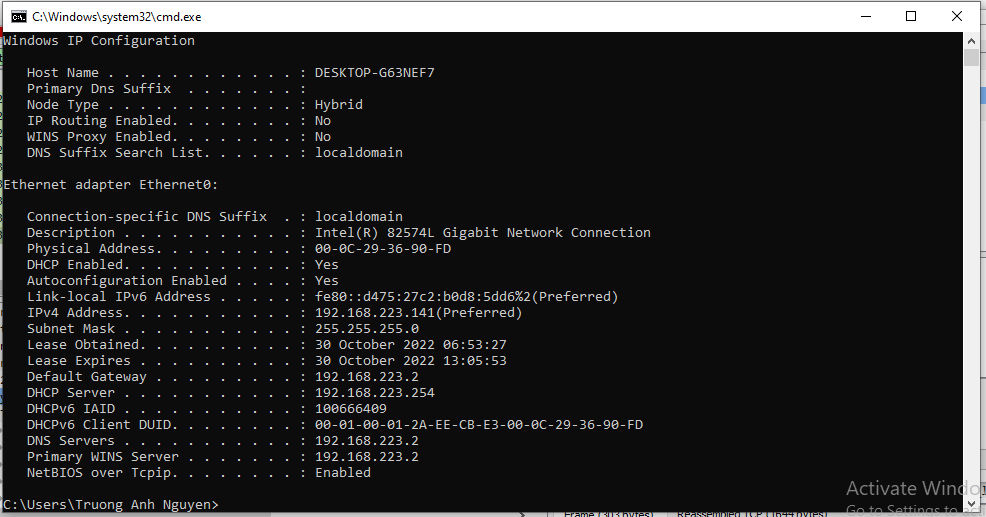
Quay trở lại máy nạn nhân để kiểm tra các địa chỉ bằng lệnh arp -a.

Lúc này địa chỉ IP của Máy nạn nhân đã trở thành địa chỉ Gateway và địa chỉ MAC trở thành địa chỉnh MAC của kẻ tấn công.



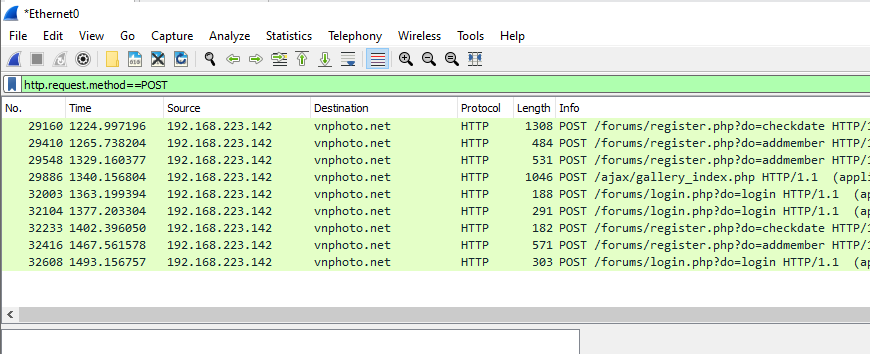
Hình 8.2.11: Địa chỉ IP và MAC của máy nạn nhân đã bị thay đổi

Quay lại máy của kẻ tấn công, kiểm tra lại địa chỉ một lần nữa bằng lệnh ipconfig /all. Lúc này địa chỉ MAC của kẻ tấn công và máy nạn nhân đã trùng nhau



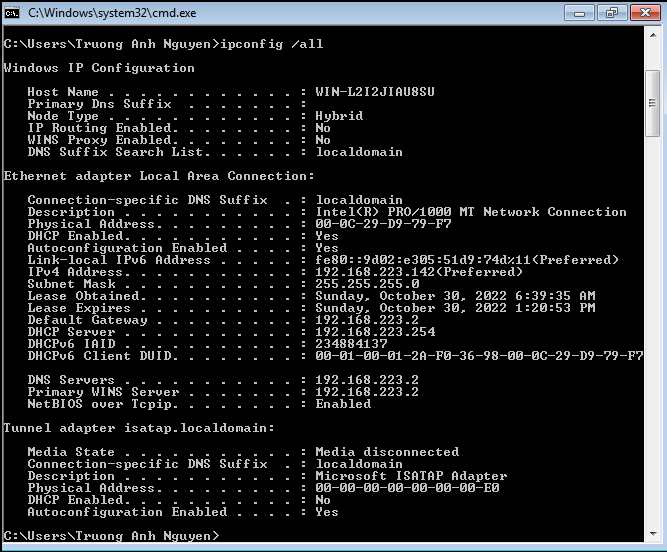
Hình 8.2.12: Địa chỉ MAC của hai máy trùng nhau

Sau đó, trên Máy tấn công chọn Capture và nhấn Stop (hoặc nhấn Ctrl + E)



Hình 8.2.13: Tắt các tính năng trên máy tấn công

Quay lại máy nạn nhân kiểm tra các địa chỉ xem có sự thay đổi không bằng lệnh ipconfig /all. Kết quả là địa chỉ MAC đã trở về là địa chỉ MAC ban đầu của máy nạn nhân.



Hình 8.2.14: Địa chỉ MAC của máy nạn nhân trở về là địa chỉ ban đầu