TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN NHẬP MÔN BẢO MẬT MÁY TÍNH**

**Nghiên cứu phát hiện nhiễm độc ARP trong mạng dựa vào Switch**

*Người hướng dẫn*: **ThS NGUYỄN QUỐC BÌNH**

*Người thực hiện*: **LÂM PHÚC NGHI – 51403239**

**NGUYỄN NHẬT TRƯỜNG – 51503103**

Lớp:

Khóa:

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2018**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN NHẬP MÔN BẢO MẬT MÁY TÍNH**

**Nghiên cứu phát hiện nhiễm độc ARP trong mạng dựa vào Switch**

Người hướng dẫn: **ThS NGUYỄN QUỐC BÌNH**

Người thực hiện: **LÂM PHÚC NGHI**

**NGUYỄN NHẬT TRƯỜNG**

Lớp **:**

Khoá  **:**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2018**

LỜI CẢM ƠN

Qua nghiên cứu, thực hiện Bài tập lớn, nhóm em đã hoàn thành.

Đầu tiên em xin cảm ơn đến Ths. Nguyễn Quốc Bình – người phụ trách môn Nhập môn bảo mật máy tính lớp lý thuyết, thầy đã tận tình giảng dạy những kiến thức cơ bản giúp chúng em có được nền tảng vững chắc để hoàn thành được phần đầu đề tài, thầy cũng là người phụ trách bài tập lớn, thầy đã tận tình giải đáp những thắc mắc về những đề tài của bài tập lớn giúp sinh viên trong việc nghiên cứu.

Em mong thầy thông cảm và góp ý, nhận xét để nhóm em có thể khắc phục được những sai sót ở các bài tập lớn/đồ án sau.

Kính chúc thầy dồi dào sức khỏe, niềm tin để tiếp tục thực hiện sứ mệnh cao đẹp của mình là truyền đạt kiến thức cho các thế hệ mai sau.

**BÀI TẬP LỚN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của ThS Nguyễn Quốc Bình;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lâm Phúc Nghi*

*Nguyễn Nhật Trường*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Tìm hiểu, trình bày về lí do ra đời của giao thức phân giải địa chỉ ARP, các thành phần trong ARP, các gói tin trong ARP, cách hoạt động của ARP. Nhược điểm của ARP, từ đó khai thác tấn công, sử dụng các phần mềm thực hiện tấn công ARP trong mạng LAN, cách phòng chống.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc531358184)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc531358185)

[TÓM TẮT iv](#_Toc531358186)

[MỤC LỤC 1](#_Toc531358187)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 4](#_Toc531358188)

[Chương 1 GIỚI THIỆU VỀ GIAO THỨC ARP. 5](#_Toc531358189)

[1.1 Đặt vấn dề. 5](#_Toc531358190)

[1.2 Giao thức ARP - Address Resolution Protocol. 5](#_Toc531358191)

[1.2.1 Định nghĩa giao thức phân giải địa chỉ - ARP. 5](#_Toc531358192)

[1.2.2 Cấu trúc gói tin ARP. 5](#_Toc531358193)

[1.2.3 Hoạt động của ARP trong mạng LAN. 8](#_Toc531358194)

[1.2.4 Các loại gói tin ARP. 9](#_Toc531358195)

[1.2.5 ARP Caching. 13](#_Toc531358196)

[1.2.6 Phân tích gói tin ARP bằng wireshark. 15](#_Toc531358197)

[Chương 2 Nguyên lý tấn công. 16](#_Toc531358198)

[2.1 Cain & abel. 17](#_Toc531358199)

[CHƯƠNG 2 – TỔNG QUAN 18](#_Toc531358200)

[1.1 Trình bày công thức toán học 18](#_Toc531358201)

[1.2 Trình bày một hình vẽ, sơ đồ 18](#_Toc531358202)

[CHƯƠNG 3 – CƠ SỞ LÝ THUYẾT / NGHIÊN CỨU THỰC NGHIỆM 20](#_Toc531358203)

[3.1 Chèn bảng: 20](#_Toc531358204)

[3.2 Viết tắt 20](#_Toc531358205)

[3.3 Trích dẫn 20](#_Toc531358206)

[3.3.1 Tài liệu tham khảo và cách trích dẫn 20](#_Toc531358207)

[3.3.2 Qui định của Khoa Công nghệ thông tin 21](#_Toc531358208)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

*f Tần số của dòng điện và điện áp (Hz)*

*p Mật độ điện tích khối (C/m3)*

**CÁC CHỮ VIẾT TẮT**

CSTD Công suất tác dụng

MF Máy phát điện

BER Tỷ lệ bít lỗi

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 2.1: Kiến trúc FTP 1](#_Toc387689394)

**DANH MỤC BẢNG**

[Bảng 3.1 Ví dụ cho chèn bảng 1](#_Toc387689363)

1. GIỚI THIỆU VỀ GIAO THỨC ARP.
   1. Đặt vấn dề.

Trong một hệ thống mạng máy tính, có hai địa chỉ được gán cho máy tính là:

- Địa chỉ logic: là địa chỉ của các giao thức mạng như IP, IPX, ... Loại địa chỉ này có thể thay đổi.

- Địa chỉ vật lý: MAC – Medium Acess Controll là dùng để định danh duy nhất, do nhà cung cấp gán cho mỗi thiết bị. Đây là loại địa chỉ phẳng, không phân lớp, nên rất khó dùng để định tuyến.

Mỗi máy tính có một card mạng, card mạng có địa chỉ MAC duy nhất. Các card mạng trong một mạng LAN liên lạc nhau thông qua địa chỉ MAC tại tần Data link (OSI).

Trong một mạng LAN, mỗi máy tính được cấp một địa chỉ IP, sử dụng ở tần Network (OSI). (Ví dụ: MAC là địa chỉ nhà, IP là tên người. Khi đặt hàng, tên người nhận hàng có thể khác mỗi lần đặt nhưng địa chỉ nhận là một).

Do đó cần cơ chế chuyển đổi 2 loại địa chỉ này với nhau. ARP được sinh ra.

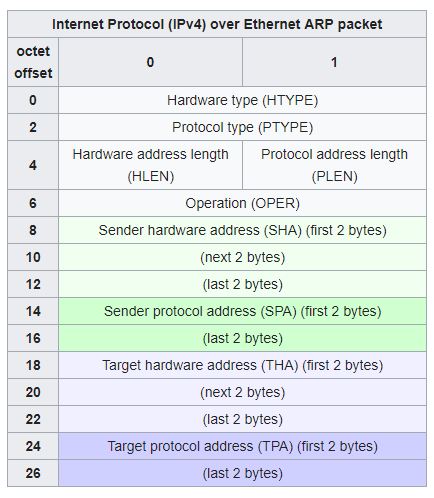
* 1. Giao thức ARP - Address Resolution Protocol.
     1. Định nghĩa giao thức phân giải địa chỉ - ARP.

ARP là phương thức phân giải địa chỉ động giữa địa chỉ lớp network và địa chỉ lớp datalink. Quá trình thực hiện bằng cách: một thiết bị IP trong mạng gửi một gói tin local broadcast đến toàn mạng yêu cầu thiết bị khác gửi trả lại địa chỉ phần cứng (địa chỉ lớp datalink) hay còn gọi là Mac Address của mình.

ARP là giao thức lớp 2 - Data link layer trong mô hình OSI và là giao thức lớp Link layer trong mô hình TCP/IP.

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 lớp hai.

* + 1. Cấu trúc gói tin ARP.

Giao thức phân giải địa chỉ sử dụng một định dạng tin nhắn đơn giản có chứa một yêu cầu địa chỉ hoặc phản hồi địa chỉ cho yêu cầu. Kích thước của gói tin ARP phụ thuộc vào kích thước của lớp liên kết (link layer) và kích thước lớp mạng (network layer). Tiêu đề tin xác định loại mạng được sử dụng ở mỗi lớp cũng như kích thước địa chỉ của mỗi lớp đó. Tiêu đề gói tin được bao gồm mã cho yêu cầu và trả lời. Gói tin bao gồm bốn địa chỉ: địa chỉ phần cứng và giao thức của máy người gửi và người nhận.

Cấu trúc gói tin ARP được hiện thị trong bảng sau, minh họa trường hợp mạng IPv4 chạy trên Ethernet. Trong trường hợp này, gói tin có các trường 48 bit cho địa chỉ phần cứng người gửi (SHA) và địa chỉ phần cứng đích (THA), các trường 32 bit cho địa chỉ giao thức người gửi và đích tương ứng (SPA và TPA). Kích thước gói tin trong trường hợp này là 28 bytes.

Hardware type: Xác định kiểu bộ giao tiếp phần cứng cần biết. Xác định với kiểu Ethernet giá trị 1.

Protocol type: Xác định kiểu giao thức cấp cao (layer 3) máy gửi sử dụng để giao tiếp. Giao thức dành cho IP có giá trị 0x0800.

Hardware address length: Xác định độ dài địa chỉ vật lý (tính theo đơn vị byte). Địa chỉ MAC nên giá trị của nó sẽ là 6.

Protocol address length: Xác định độ dài địa chỉ logic được sử dụng ở tầng trên (layer 3). Tùy thuộc vào IP sử dụng mà có giá trị khác nhau, hiện tại IPv4 được sử dụng rộng rãi nên trường này sẽ có giá trị là 4 (byte).

Operation code: Xác định loại gói tin ARP mà máy gửi gửi. Có một số giá trị phổ biến:

1 : gói tin ARP request.

2 : gói tin ARP rely.

3 : gói tin RARP request.

4 : gói tin RARP reply.

Sender hardware address (SHA): Xác định địa chỉ MAC máy gửi.

Trong gói tin ARP request: trường này xác định địa chỉ MAC của host gửi request.

Trong gói tin ARP reply: trường này xác định địa chỉ MAC của máy host mà máy gửi bên trên muốn tìm kiếm.

Sender protocol address (SPA): Xác định địa chỉ IP máy gửi.

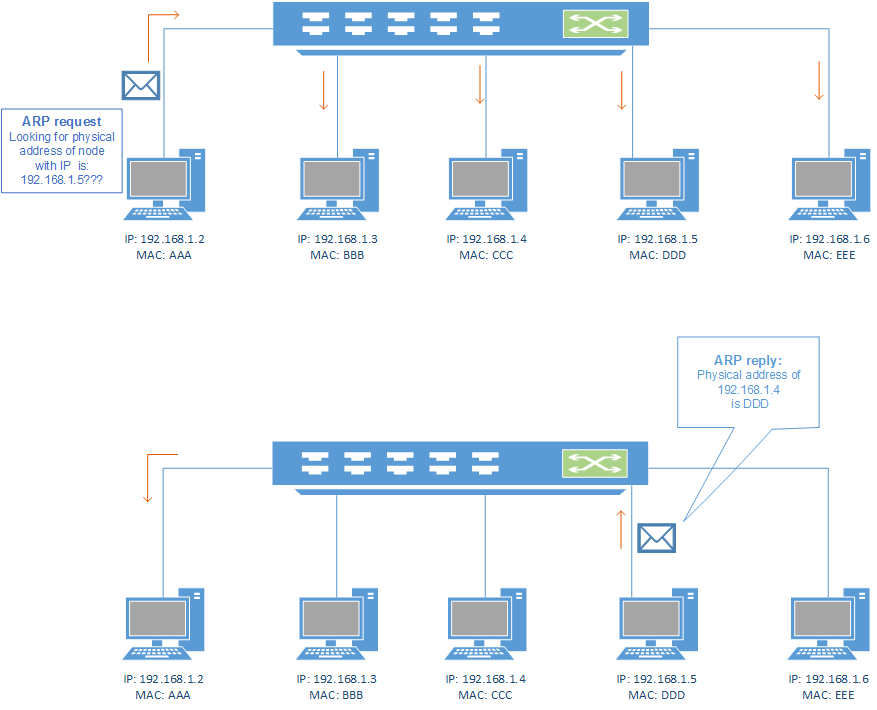
Target hardware address (THA): Xác định địa chỉ MAC máy nhận mà máy gửi cần tìm.

Trong gói tin ARP request: Trường này chưa được xác định (nên sẽ để giá trị là: 00:00:00:00:00:00)

Trong gói tin ARP reply: Trường này sẽ điền địa chỉ của máy gửi gói tin ARP request.

Target protocol address (PTA): Xác định địa chỉ IP máy gửi (máy cần tìm).

* + 1. Hoạt động của ARP trong mạng LAN.



Bước 1: Máy gửi kiểm tra cache của mình. Nếu đã có thông tin về sự ánh xạ giữa địa chỉ IP và địa chỉ MAC thì chuyển sang Bước 7.

Bước 2: Máy gửi khởi tạo gói tin ARP request với địa chỉ SHA và SPA là địa chỉ của nó, và địa chỉ TPA là địa chỉ IP của máy cần biết MAC. (Trường THA để giá trị toàn 0 để biểu hiện là chưa tìm được địa chỉ MAC)

Bước 3: Gửi quảng bá gói tin ARP trên toàn mạng (Địa chỉ MAC đích của gói tin Ethernet II là địa chỉ MAC quảng bá ff:ff:ff:ff:ff:ff).

Bước 4: Các thiết bị trong mạng đều nhận được gói tin ARP request. Gói tin được xử lý bằng cách các thiết bị đều nhìn vào trường địa chỉ Target Protocol Address.

Các thiết bị không trùng địa chỉ TPA thì hủy gói tin.

Thiết bị với IP trùng với IP trong trường Target Protocol Address sẽ bắt đầu quá trình khởi tạo gói tin ARP Reply bằng cách lấy các trường Sender Hardware Address và Sender Protocol Address trong gói tin ARP nhận được đưa vào làm Target trong gói tin gửi đi. Đồng thời thiết bị sẽ lấy địa chỉ MAC của mình để đưa vào trường Sender Hardware Address. Đồng thời cập nhất giá trị ánh xạ địa chỉ IP và MAC của máy gửi vào bảng ARP cache của mình để giảm thời gian xử lý cho các lần sau.

Bước 5: Thiết bị đích bắt đầu gửi gói tin Reply đã được khởi tạo đến thiết bị nguồn vừa gửi gói tin ARP request. Gói tin reply là gói tin gửi unicast.

Bước 6: Thiết bị nguồn nhận được gói tin reply và xử lý bằng cách lưu trường Sender Hardware Address trong gói reply như địa chỉ phần cứng của thiết bị đích cần tìm.

Bước 7: Thiết bị nguồn update vào ARP cache của mình giá trị tương ứng giữa địa chỉ IP và địa chỉ MAC của thiết bị đích. Lần sau sẽ không còn cần tới ARP request.

* + 1. Các loại gói tin ARP.

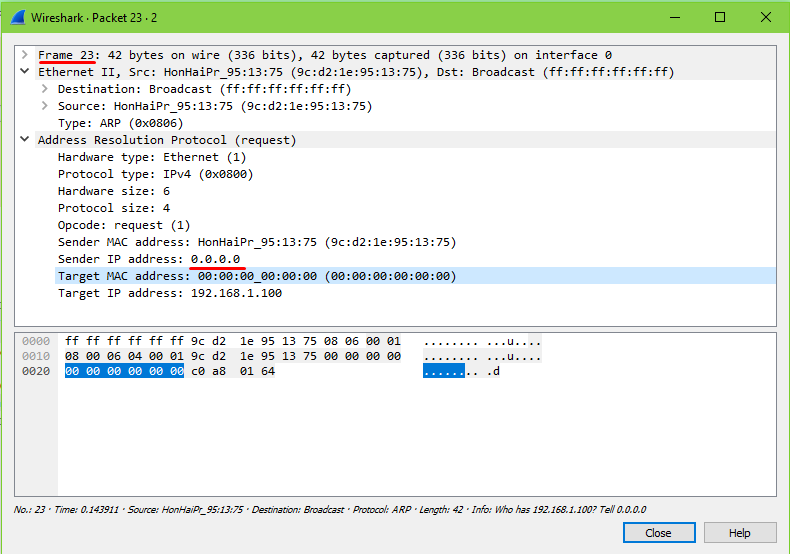
ARP probe: Đây là loại tin ARP dùng để máy thăm dò xem địa chỉ mà máy được cấp phát (cấu hình manual hoặc DHCP, ...) có bị trùng với địa chỉ IP của máy nào trong cùng mạng hay không. Khi mới ban đầu, các máy đều thực hiện broadcast gói tin ARP này.

Loại tin này có cấu trúc địa chi IP của máy gửi là 0.0.0.0 (thể hiện máy gửi gói tin này chưa xác định IP, đồng thời cũng là để các máy khác trong mạng không cập nhật MAC của máy vào ARP caching - vì nó chưa được gán IP cụ thể nào)

Địa chỉ MAC đích là 00:00:00:00:00:00

Địa chỉ IP đích là địa chỉ IP mà máy gửi được cấp phát.

Thông thường loại tin ARP request này sẽ không có reply.

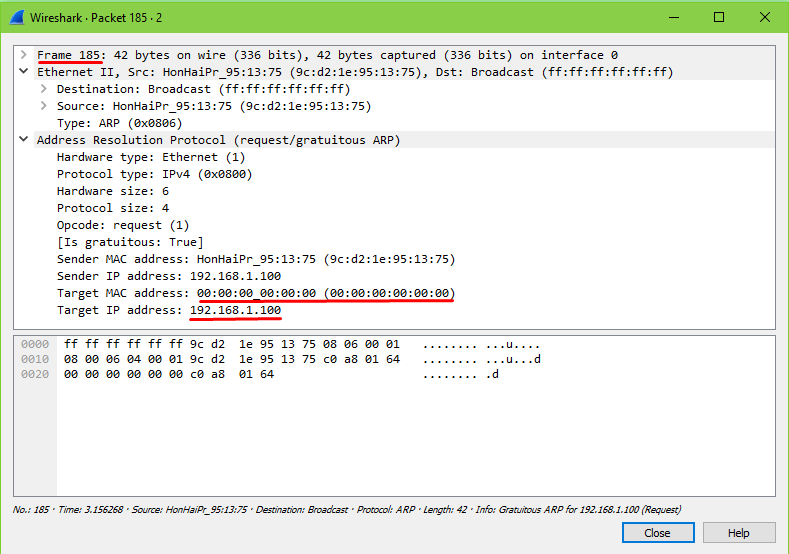


Hình minh họa: Gói tin ARP probe bắt được từ wireshark.

ARP announcements: ARP cũng sử dụng một cách đơn giản để thông báo tới các máy trong mạng khi địa chỉ IP hoặc địa chỉ MAC của nó thay đổi. Đó chính là loại tin gratuitous ARP.

Gói tin Gratuitous ARP được gửi broadcast request trong mạng với địa chỉ MAC và IP máy gửi là địa chỉ sau khi thay đổi.

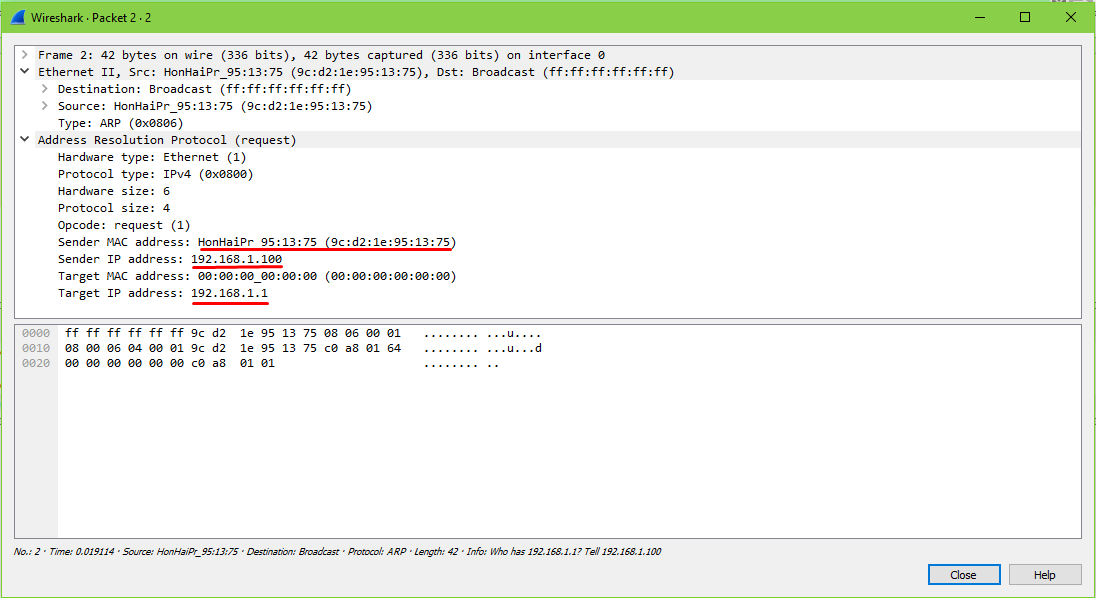
Địa chỉ MAC đích là 00.00.00.00.00.00. Địa chỉ IP đích là chính nó. Điều này đảm bảo các máy trong mạng khi nhận được gói tin này sẽ chỉ cập nhật địa chỉ MAC và IP của máy gửi vào trong ARP caching của mình => không có gói tin reply cho gói tin này.



Hình minh họa: Gói tin Gratuitous ARP bắt được từ Wireshark.

ARP request: Là loại tin ARP request mà máy gửi gửi broadcast để tìm địa chỉ MAC của máy nhận.

Địa chỉ MAC và IP gửi là địa chỉ của máy gửi. Địa chỉ MAC nhận được set là 0 hết. Địa chỉ IP nhận là địa chỉ IP của máy cần tìm.



Hình minh họa: Một gói tin request của máy 192.168.1.100 tìm MAC của gateway trong mạng: 192.168.1.1.

ARP reply: Là loại tin mà máy nhận sau khi nhận được ARP request sẽ đóng gói lại MAC của mình và gửi gói tin reply về cho máy gửi. Nó sẽ đóng gói là địa chỉ IP và MAC của mình vào địa chỉ SHA và PHA. Địa chỉ mà máy gửi gửi tới nó sẽ được đóng gói và phần địa chỉ THA và TPA. Gửi gói tin unicast.



Hình minh họa: Gói tin do gateway gửi địa chỉ MAC của mình về cho máy 192.168.1.100 trong mạng.

* + 1. ARP Caching.

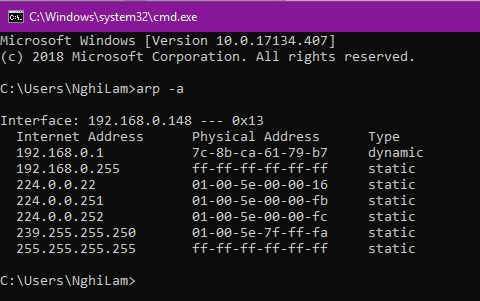
ARP là một giao thức phân giải địa chỉ động. Quá trình gửi gói tin Request và Reply sẽ tiêu tốn băng thông mạng. Chính vì vậy càng hạn chế tối đa việc gửi gói tin Request và Reply sẽ càng góp phần làm tăng khả năng họat động của mạng.

=> Từ đó sinh ra nhu cầu của ARP Caching.

Ngoài việc làm giảm lưu lượng mạng, ARP cache cũng đảm bảo độ phân giải các địa chỉ thường dùng là nhanh chóng, đảm bảo hiệu suất hoạt động tổng thể của mạng.

ARP Cache có dạng giống như một bảng tương ứng giữa địa chỉ hardware và địa chỉ IP.

(Trong Window: dùng câu lệnh arp -a trong Command Prompt để show ra ARP cache trong máy)



Có hai cách đưa các thành phần tương ứng vào bảng ARP :

Static ARP Cache Entries: Đây là cách mà các thành phần tương ứng trong bảng ARP được đưa vào lần lượt bởi người quản trị. Công việc được tiến hành một cách thủ công.

Sử dụng trong trường hợp mà các workstation nên có static ARP entry đến router và file server nằm trong mạng. Điều này sẽ hạn chế việc gửi các gói tin để thực hiện quá trình phân giải địa chỉ.

Sử dụng câu lệnh arp -s ip\_addr mac\_addrđể thêm một Static ARP entri vào ARP cache.

Nhược điểm: ngoài hạn chế của việc phải nhập bằng tay, static cache còn thêm hạn chế nữa là khi địa chỉ IP của các thiết bị trong mạng thay đổi thì sẽ dẫn đến việc phải thay đổi ARP cache.

Dynamic ARP Cache Entries: Đây là quá trình mà các thành phần địa chỉ hardware/IP được đưa vào ARP cache một cách hoàn toàn tự động bằng phần mềm sau khi đã hoàn tất quá trình phân giải địa chỉ.

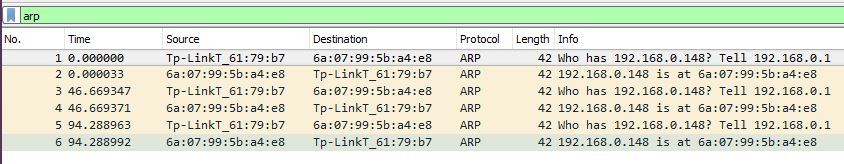
Chúng được lưu trong cache trong một khoảng thời gian và sau đó sẽ được xóa đi.

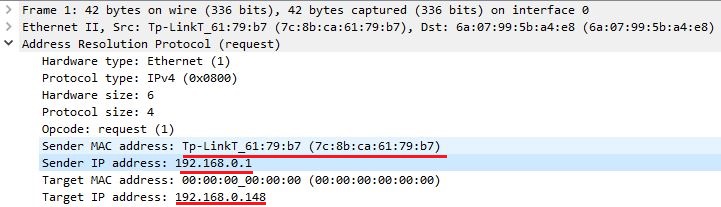
Dynamic Cache được sử dụng rộng rãi hơn vì tất cả các quá trình diễn ra tự động và không cần đến sự tương tác của người quản trị.

Trong môi trường mạng thực tế, có nhiều lý do tác động dẫn tới sự ảnh hưởng làm thay đổi các thông tin về việc ánh xạ IP và MAC nên các thông tin trong dynamic cache sẽ được tự động xóa sau một khoảng thời gian nhất định. Quá trình này được thực hiện một cách hoàn toàn tự động khi sử dụng ARP với khoảng thời gian thường là 10 hoặc 20 phút (hoặc lâu hơn tùy vào loại thiết bị mà mình sử dụng, phụ thuộc nhà cung cấp). Sau một khoảng thời gian nhất định được lưu trong cache , thông tin sẽ được xóa đi. Lần sử dụng sau, thông tin sẽ được update trở lại. (đây là lúc mà các gói tin ARP announcements phát huy tác dụng).

* + 1. Phân tích gói tin ARP bằng wireshark.

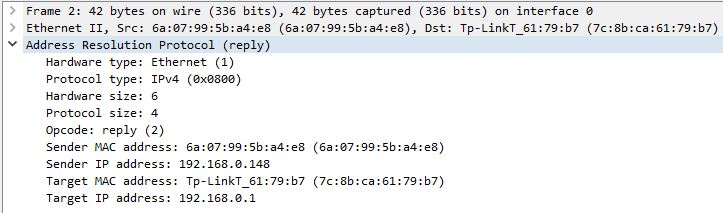
Lọc các gói tin ARP.





Gói tin số 1 là gói tin ARP request mà máy gửi (192.168.0.1) hỏi để tìm MAC của gateway.

Gói tin số 2 là gói tin ARP reply mà gateway trả về.



1. Nguyên lý tấn công.

Trong giao thức ARP không có cơ chế xác thực quá trình phân giải. Một máy khi nhận được gói tin arp reply nó chỉ sử dụng địa chỉ MAC có trong gói tin đó. Từ đó dẫn đến kiểu tấn công Man in the middle (MITM).

MITM: máy tấn công (H) cùng mạng nội bộ với máy nạn nhân (V) muốn nghe lén thông tin của máy V với một máy X khác (máy X này cùng mạng hoặc khác mạng, khác mạng thì qua router).

Bước 1: kẻ tấn công sẽ gửi gói tin ARP Reply đến máy V với nội dung là địa chỉ MAC của H và địa chỉ IP của X.

Bước 2: kẻ tấn công gửi gói tin ARP Reply đến Z với nội dung là địa chỉ MAC của H và địa chỉ IP của X.

Bước 3: Máy H sẽ enable chức năng IP forwarding nhằm giúp cho các gói tin qua lại giữa X và V vẫn được đến với nhau.

Khi đó, mọi thông tin giữa V và X đều đi qua H và bị ghi lại.

Sử dụng phần mềm cho tấn công: Cain & abel.

Denial of services:

Máy từ bên tấn công gửi gói ARP reply đến tất cả các máy trong mạng với nội dung là IP gateway và MAC giả. Lúc này toàn bộ các máy trong mnajng không thể liên lạc với các mạng khác (internet).

Phần mềm: netcut.

Mac flooding: bên tấn công gửi liên tục các gói tin ARP reply, switch sẽ xử lý không kịp hoặc chậm. Do đó, làm chậm tốc độ vận tải của mạng và bị đánh cắp thông tin.

Biện pháp phòng chống: trong mô hình mạng nhỏ sử dụng ARP tĩnh. Trong mô hình mạng lớn, sử dụng post security, arp watch, wireshark.

* 1. Cain & abel.

**TÀI LIỆU THAM KHẢO**

1. http://luanvan.net.vn/luan-van/de-tai-tim-hieu-va-thuc-hien-tan-cong-arp-spoofing-va-sniffer-31123/
2. <https://github.com/hocchudong/thuctap012017/blob/master/TamNT/T%C3%ACm%20hi%E1%BB%83u%20giao%20th%E1%BB%A9c%20ARP.md>
3. <https://viblo.asia/p/tim-hieu-giao-thuc-arprarp-trong-bo-giao-thuc-tcpip-mPjxMeZKG4YL>
4. <http://www.vnpro.org/forum/forum/cclabpro/ccnp-labpro-ccnp-switching/27559-arp-attack-c%C6%A1-ch%E1%BA%BF-t%E1%BA%A5n-c%C3%B4ng-v%C3%A0-c%C3%A1ch-ph%C3%B2ng-ch%E1%BB%91ng>
5. <https://security.stackexchange.com/questions/91170/how-to-simulate-network-attacks-and-use-wireshark-to-detect-them>
6. http://www.academia.edu/5648727/ARP\_Spoofing-\_Analysis\_using\_Wireshark\_on\_2\_different\_OS\_LINUX\_and\_WINDOWS

**PHỤ LỤC**