

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



THỰC TẬP CƠ SỞ

Đề tài:

Xây dựng chương trình phát hiện hình thức tấn công ARP Cache Poisoning

Giảng viên hướng dẫn: TS. HUỖNH TRỌNG THƯA
Ths. HUỖNH THANH TÂM

Sinh viên thực hiện:

Lớp	D19CQAT01-N
Trương Chí Tài	N19DCAT067
Nguyễn Thế Bảo	N19DCAT007
Từ Nguyễn Quốc Huy	N19DCAT038
Nguyễn Minh Thuận	N19DCAT086
Phan Thị Nguyệt Nhi	N19DCAT058
Lê Minh Đức	N19DCAT017

TP.HCM, tháng 3/2022

LỜI CẢM ƠN

Đầu tiên, nhóm em xin gửi lời cảm ơn chân thành đến tất cả thầy cô đã giảng dạy và cho chúng em những kiến thức vô cùng quan trọng và quý báu của mình trong quá trình học tập tại Học Viện để chúng em có những kỹ năng và những kiến thức cần thiết để hoàn thành đề tài này.

Đặc biệt, nhóm em xin vô cùng biết ơn thầy TS. Huỳnh Trọng Thừa và thầy Ths. Huỳnh Thanh Tâm đã tận tình hướng dẫn, truyền đạt những kiến thức và kinh nghiệm của thầy và dạy bảo chúng em trong quá trình học tập và thực hiện đề tài này. Xin chúc gia đình hai thầy có thật nhiều sức khỏe và thành công trong cuộc sống. Từ đó mang đến cho chúng em và các bạn sau này những kiến thức và kinh nghiệm quý báu của thầy.

Cảm ơn tất cả những người bạn đã ít nhiều cho mình những kiến thức và hiểu biết của mình, luôn đồng hành và sát cánh cùng mình trong quá trình học tập và rèn luyện các kỹ năng. Quan trọng hơn cả là động lực và niềm vui mà mình chắc chỉ có các bạn mới có thể mang lại. Từ đó mình có thể vượt qua những khó khăn và áp lực trong học tập cũng như trong cuộc sống.

Đề tài đã được nhóm chúng em hoàn thành đúng tiến độ. Tuy nhiên, nhóm em vẫn còn nhiều thiếu sót do chưa có nhiều kinh nghiệm. Mong thầy cô chỉ bảo, đóng góp ý kiến để chúng em có nhiều hơn những kiến thức và kỹ năng để hoàn thành tốt công tác nghiên cứu, làm việc sau này cũng như trong cuộc sống. Một lần nữa chúng em xin cảm ơn thầy cô rất nhiều.

TP.HCM, ngày 12 tháng 3 năm 2022

Đại diện nhóm thực hiện

Trương Chí Tài

MỤC LỤC

LỜI CẢM ƠN.....	1
MỤC LỤC.....	2
LỜI MỞ ĐẦU.....	4
CHƯƠNG 1. CƠ SỞ LÝ THUYẾT.....	5
1.1 Giới thiệu về ARP.....	5
1.1.1 ARP là gì?.....	5
1.1.2 Các loại ARP:.....	5
1.1.3 Lịch sử và mục đích:.....	5
1.1.4 Cơ chế hoạt động:.....	6
1.1.5 Các loại bản tin:.....	6
1.1.6 Các bước hoạt động của giao thức ARP:.....	8
1.2 Cơ chế tấn công ARP Cache Poisoning.....	9
1.2.1 ARP Cache Poisoning là gì?.....	9
1.2.2 Các bước tấn công:.....	9
1.2.3 Hậu quả:.....	10
1.2.4 Phương pháp phát hiện:.....	11
1.2.5 Biện pháp phòng chống:.....	12
CHƯƠNG 2. THIẾT KẾ VÀ XÂY DỰNG CHƯƠNG TRÌNH.....	12
2.1 Giới thiệu chương trình:.....	12
2.2 Thực hiện:.....	12
2.2.1 Giải thuật phát hiện ARP Cache Poisoning:.....	12
2.2.2 Cảnh báo trên giao diện:.....	13
2.2.3 Cảnh báo qua âm thanh:.....	13
2.2.4 Cảnh báo qua email:.....	13
CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM.....	13
3.1 Kịch bản 1: Sử dụng Ettercap trên máy Kali thực hiện ARP Poisoning và xem cấu hình thiết bị khi telnet của người dùng:.....	13

3.2 Kịch bản: Sử dụng Ettercap trên máy Kali thực hiện ARP Poisoning và thông tin của các gói tin(thông tin tài khoản và mật khẩu) khi người dùng truy cập các trang web sử dụng giao thức HTTP:	16
3.3 Sử dụng chương trình để phát hiện tấn công:	18
KẾT LUẬN:	20
- <i>Kết quả:</i>	20
- <i>Hạn chế:</i>	20
- <i>Hướng phát triển:</i>	20
TÀI LIỆU THAM KHẢO:	21

LỜI MỞ ĐẦU

Hiện nay, dù các cuộc tấn công ARP Cache Poisoning đã được các kẻ tấn công thực hiện từ rất lâu và vẫn tồn tại đến ngày nay trong các cuộc tấn công mạng cục bộ và cho phép kẻ tấn công âm thầm nghe trộm hoặc thao tác tất cả các dữ liệu bạn gửi qua mạng một cách dễ dàng nếu dữ liệu của chúng ta không được mã hóa. Dữ liệu này bao gồm tài liệu, email,... Tấn công ARP không bị phát hiện bởi firewall và các tính năng bảo mật của hệ điều hành: firewall không bảo vệ chúng ta khỏi các cuộc tấn công ARP. Vì thế là các sinh viên an toàn thông tin, chúng em có trách nhiệm nghiên cứu và phát triển các phần mềm giám sát để phát hiện các cuộc tấn công mạng và các hành động truy cập hệ thống trái phép như tấn công ARP Cache Poisoning,... Để thực hiện đề tài này chúng em sẽ tìm hiểu về các cơ sở lý thuyết như giao thức ARP là gì, cách giao thức hoạt động và điểm yếu để các kẻ tấn công lợi dụng để tấn công, cách phát hiện và phòng chống, từ đó thiết kế chương trình bằng Java để phát hiện khi bị tấn công ARP Poisoning.

CHƯƠNG 1. CƠ SỞ LÝ THUYẾT

1.1 Giới thiệu về ARP

1.1.1 ARP là gì?

- ARP (Address Resolution Protocol) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network. Thiết bị gửi sử dụng ARP để có thể dịch địa chỉ IP sang địa chỉ MAC. Thiết bị sẽ gửi một request ARP đã chứa địa chỉ IP của thiết bị nhận. Tất cả thiết bị trên đoạn local network sẽ nhìn thấy thông điệp này. Tuy nhiên, chỉ thiết bị có địa chỉ IP chứa trong request mới có thể phản hồi lại với thông điệp mà chứa địa chỉ MAC của nó. Thiết bị gửi khi đó sẽ có đầy đủ các thông tin để gửi packet tới thiết bị nhận.

1.1.2 Các loại ARP:

- ARP được phân thành 4 loại chính: Proxy ARP, Gratuitous ARP, Reverse ARP, Inverse ARP.

Proxy ARP

Trong phương pháp Proxy ARP, các thiết bị Layer 3 có thể phản hồi các ARP request. Loại ARP này được cấu hình sao cho router sẽ phản hồi địa chỉ IP đích, và ánh xạ địa chỉ MAC đến địa chỉ IP đích và người gửi khi nó đến được đích.

Gratuitous ARP

Gratuitous ARP là một loại ARP request khác của host. Loại request này giúp mạng có thể xác định các địa chỉ IP bị trùng lặp. Do đó, khi router hay switch gửi ARP request để lấy địa chỉ IP, nó sẽ không nhận được phản hồi ARP nào. Vì vậy cũng không có node nào có thể sử dụng địa chỉ IP được cấp cho router hay switch đó.

Reverse ARP (RARP)

Reverse ARP (RARP) là một loại giao thức ARP được hệ thống client trong LAN sử dụng để yêu cầu địa chỉ IPv4 của nó từ bảng ARP router. Quản trị viên mạng chủ yếu tạo một bảng trong bộ gateway-router, giúp xác định địa chỉ MAC đến IP cụ thể.

Inverse ARP (InARP)

InARP là một loại ARP dùng để tìm địa chỉ IP của các node từ địa chỉ lớp liên kết dữ liệu. InARP được sử dụng rộng rãi cho các rơ-le frame mạng ATM, trong đó địa chỉ mạch ảo Lớp 2 thu được từ việc signal của Layer 2.

1.1.3 Lịch sử và mục đích:

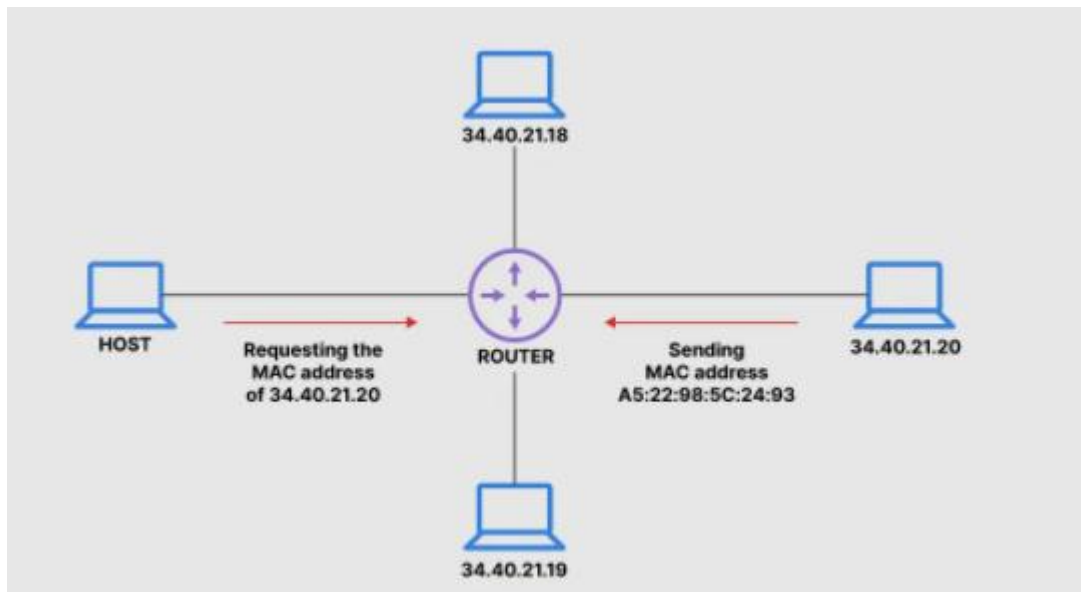
- ARP được hình thành và phát triển vào đầu những năm 1980 như một giao thức dịch địa chỉ chung cho các mạng IP. Bên cạnh Ethernet và WiFi thì ARP đã được triển khai cho ATM, Token Ring và cả những loại mạng vật lý khác.

- ARP cho phép một mạng quản lý các kết nối độc lập với những thiết bị vật lý cụ thể được gắn vào từng mạng. Điều này cho phép giao thức Internet vận hành hiệu

quá hơn so với việc nó phải tự quản lý địa chỉ của các thiết bị phần cứng và mạng vật lý.

1.1.4 Cơ chế hoạt động:

Quá trình hoạt động của ARP được bắt đầu khi một thiết bị nguồn trong một mạng IP có nhu cầu thực hiện gửi một gói tin IP. Trước hết thiết bị đó phải xác định được xem địa chỉ IP đích của gói tin có phải đang nằm cùng trong mạng nội bộ của mình hay không. Nếu đúng vậy thì thiết bị sẽ thực hiện gửi trực tiếp gói tin đến thiết bị đích. Nếu địa chỉ IP đích đang nằm trên mạng khác, thì thiết bị sẽ gửi gói tin đến một trong các router nằm cùng ở trên mạng nội bộ để router này làm nhiệm vụ forward gói tin.



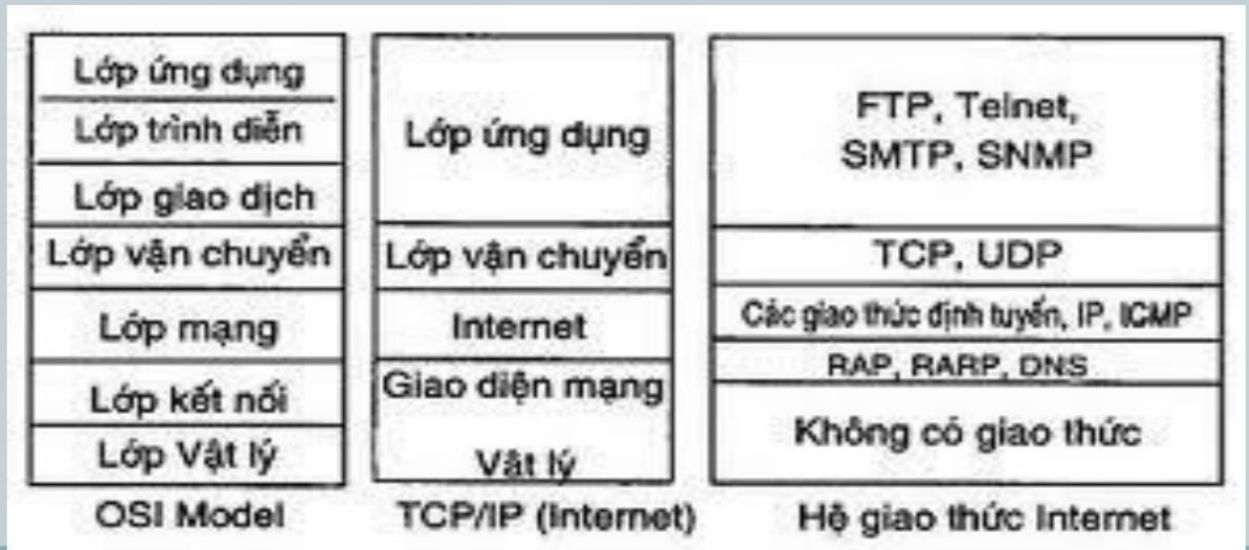
Cả hai trường hợp, bạn đều thấy được là thiết bị phải gửi gói tin IP đến một thiết bị IP khác trên cùng mạng nội bộ. Chúng ta biết rằng việc gửi gói tin trong cùng mạng thông qua Switch là dựa vào địa chỉ MAC hay là địa chỉ phần cứng của thiết bị. Sau khi gói tin được đóng gói thì hệ thống mới bắt đầu được chuyển qua quá trình phân giải địa chỉ ARP và thực hiện chuyển đi.

ARP về cơ bản là một quá trình có 2 chiều request/response giữa các thiết bị trong cùng mạng nội bộ. Thiết bị nguồn request bằng cách gửi một bản tin local broadcast lên trên toàn mạng. Thiết bị đích response bằng một bản tin unicast để trả lại cho thiết bị nguồn.

1.1.5 Các loại bản tin:

* Có hai dạng bản tin trong ARP cơ bản nhất: một là được gửi từ nguồn đến đích, còn một là được gửi từ đích tới nguồn.

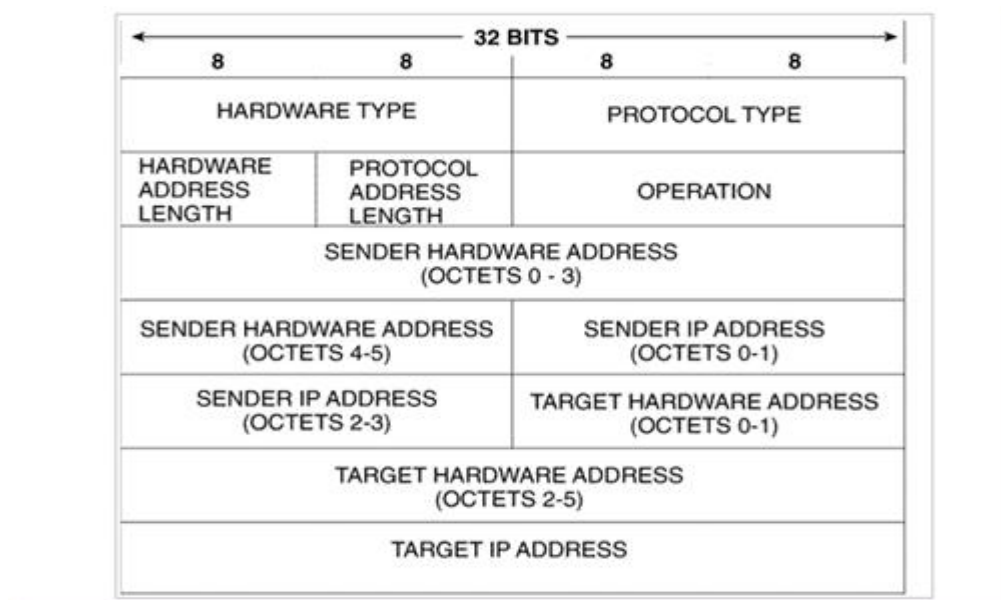
Vị trí của ARP:



- Request: Khi hệ thống khởi tạo quá trình, gói tin được gửi từ máy nguồn tới thiết bị đích.
- Reply: Khi quá trình đáp trả gói tin ARP request, được gửi từ thiết bị đích đến máy nguồn.

* Có 4 loại địa chỉ nằm trong một bản tin ARP đó là:

- Sender Hardware Address: Đây là địa chỉ lớp hai của thiết bị gửi bản tin.
- Sender Protocol Address: Đây là địa chỉ lớp ba (hay còn gọi là địa chỉ logic) của thiết bị gửi bản tin.
- Target Hardware Address: Địa chỉ lớp hai (hay còn được gọi là địa chỉ phần cứng) của thiết bị đích của bản tin.
- Target Protocol Address: Địa chỉ lớp ba (hay gọi là địa chỉ logic) của thiết bị đích của bản tin.



1.1.6 Các bước hoạt động của giao thức ARP:

Bước 1: Source Device Checks Cache: Trong bước này, thiết bị sẽ thực hiện kiểm tra cache (bộ đệm) của mình. Nếu đã có địa chỉ IP đích tương ứng với MAC nào đó rồi thì lập tức hệ thống chuyển sang bước 9.

Bước 2: Source Device Generates ARP Request Message: Hệ thống bắt đầu khởi tạo gói tin ARP Request với các trường địa chỉ như trên.

Bước 3: Source Device Broadcasts ARP Request Message: Thiết bị nguồn truyền gói tin ARP Request trên toàn mạng.

Bước 4: Local Devices Process ARP Request Message: Các thiết bị trong mạng đều sẽ nhận được gói tin ARP Request. Gói tin được xử lý bằng cách đưa thiết bị vào trường địa chỉ Target Protocol Address. Nếu trùng với địa chỉ của mình thì tiếp tục xử lý, nếu không thì hủy gói tin.

Bước 5: Destination Device Generates ARP Reply Message: Nếu Thiết bị với IP trùng với IP trong trường Target Protocol Address sẽ thực hiện quá trình khởi tạo gói tin ARP Reply. Đồng thời thiết bị sẽ lấy địa chỉ datalink của mình để tiến hành đưa vào trường Sender Hardware Address.

Bước 6: Destination Device Updates ARP Cache: Thiết bị đích cập nhật bảng ánh xạ địa chỉ IP và MAC của thiết bị nguồn vào bảng ARP cache của mình để giảm bớt thời gian xử lý cho những lần sau.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a

Interface: 10.10.10.1 --- 0xb
Internet Address      Physical Address      Type
10.10.10.2            00-50-56-c0-00-01    dynamic
10.10.10.255          ff-ff-ff-ff-ff-ff    static
192.168.137.1         00-50-56-c0-00-01    dynamic
192.168.137.254       00-50-56-f3-54-3f    dynamic
224.0.0.22            01-00-5e-00-00-16    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

C:\Windows\system32>netsh interface ip delete arpcache
Ok.

C:\Windows\system32>_
```

Bước 7: Destination Device Sends ARP Reply Message: Thiết bị đích sẽ bắt đầu gửi gói tin Reply đã được khởi tạo đến thiết bị nguồn.

Bước 8: Source Device Processes ARP Reply Message: Thiết bị nguồn nhận được gói tin reply và tiến hành xử lý bằng cách lưu trường Sender Hardware Address trong gói reply như những địa chỉ phần cứng của thiết bị đích

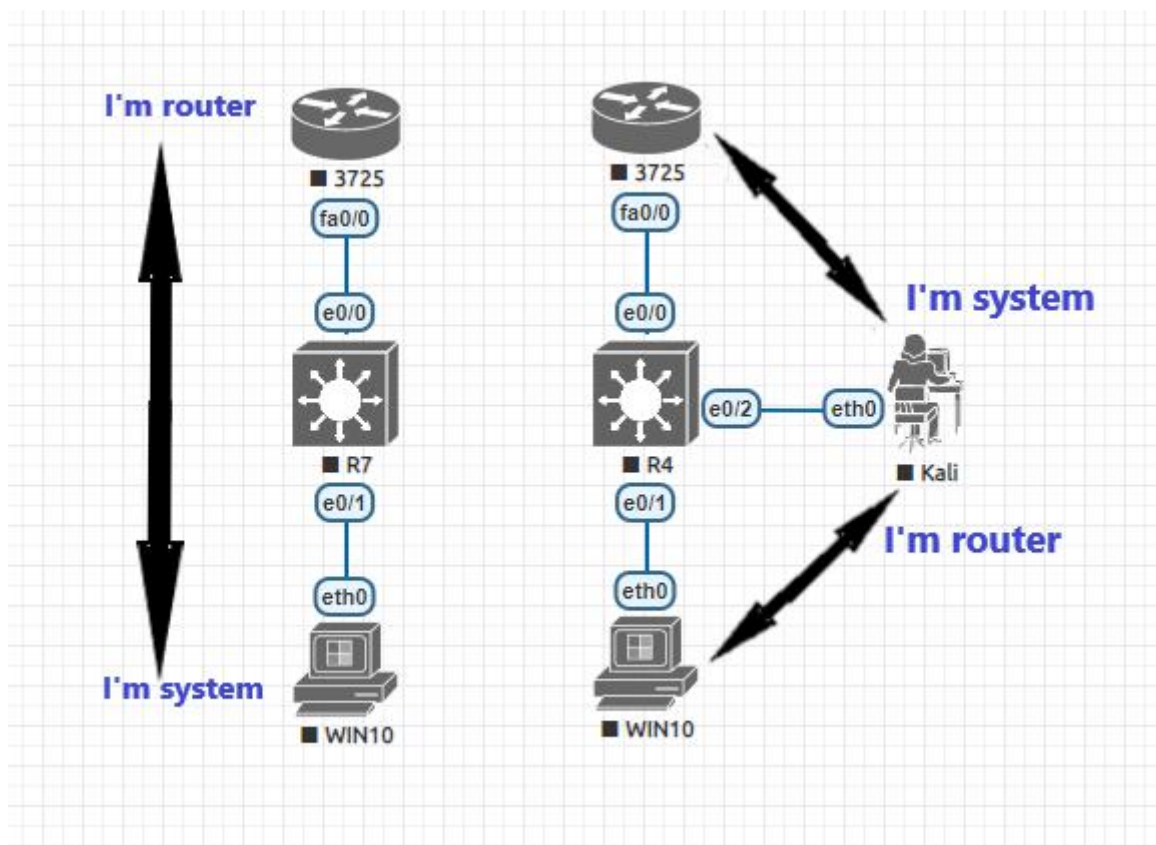
Bước 9: Source Device Updates ARP Cache: Thiết bị nguồn update vào ARP cache giá trị tương ứng giữa địa chỉ network và cả địa chỉ datalink của thiết bị đích. Do đó, những lần tiếp theo sẽ không còn cần tới request.

1.2 Cơ chế tấn công ARP Cache Poisoning

1.2.1 ARP Cache Poisoning là gì?

- **ARP Cache Poisoning** là một cuộc tấn công Man in the Middle (MitM) cho phép những kẻ tấn công chặn giao tiếp giữa các thiết bị mạng. Kẻ tấn công giả thông điệp ARP trong mạng cục bộ. Nói chung, mục tiêu là kết hợp địa chỉ MAC của kẻ tấn công với địa chỉ IP của máy chủ khác, chẳng hạn như cổng mặc định (default gateway), làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công.

1.2.2 Các bước tấn công:



- Hai máy A và B sẽ thực hiện truyền thông bình thường với giao thức ARP như cơ chế đã trình bày ở trên
- Khi muốn truyền thông tin giữa hai máy A và B thì hai máy sẽ tra thông tin IP và MAC của máy đích trong bảng ARP. Nếu không thấy thì máy sẽ gửi ARP request để hỏi MAC của máy đích.
- Dựa theo đó, Attacker liên tục thực hiện gửi các gói ARP Reply nhằm đầu độc bộ đệm ARP Cache của máy gửi request. Nó khiến cho máy gửi request hiểu lầm rằng IP của máy đích có MAC tương ứng là MAC của Attacker. Tương tự, Attacker cũng sẽ làm vậy với máy còn lại.
- Sau khi đầu độc, kẻ tấn công có thể lấy cắp được thông tin cơ mật của hai máy A và B. Vì lúc này dữ liệu truyền thông giữa hai máy đều sẽ đi qua máy Attacker trước khi đi đến được máy đích.

1.2.3 Hậu quả:

- Attacker có thể đứng ở giữa bắt các gói tin truyền giữa 2 thiết bị, trừ khi các gói đã đã được mã hóa thông qua một kênh nào đó như HTTPS, SSH.
- **Session Hijacking:** Các cuộc tấn công Session Hijacking có bản chất tương tự như Man-in-the-Middle, ngoại trừ việc kẻ tấn công sẽ không chuyển tiếp trực tiếp lưu lượng truy cập từ máy nạn nhân đến đích dự kiến của nó. Thay vào đó, kẻ tấn công sẽ nắm bắt số thứ tự TCP chính hãng hoặc web cookie từ nạn nhân và sử dụng nó để giả danh tính của nạn nhân. Ví dụ: điều này có thể được sử dụng để truy cập

tài khoản mạng xã hội của người dùng mục tiêu nếu họ tình cờ đăng nhập. Vì khi bắt được các gói tin không mã hóa, nên attacker có thể lấy được session ID, và chiếm quyền truy cập vào tài khoản máy nạn nhân vừa truy cập.

- Thay đổi các gói tin rồi mới chuyển đi tiếp: ví dụ gửi một file độc hại hay một website giả mạo đến máy trạm, nhiều tool như Ettercap cho phép attacker trở thành proxy hay người xem, và sửa đổi thông tin trước khi chuyển đến đích luôn, kết hợp với DNS Poisoning thì cuộc tấn công sẽ trở nên hiệu quả hơn, ví dụ nạn nhân truy cập đến một website của một trang web có tên miền quen thuộc nhưng nó lại có IP của máy attacker thay vì IP thực sự của website đó.

- **DDoS (Distributed Denial of Service):** Một cuộc tấn công DDoS nhằm từ chối một hoặc nhiều nạn nhân truy cập vào tài nguyên mạng. Trong trường hợp ARP, kẻ tấn công có thể gửi ARP reply ánh xạ sai hàng trăm hoặc thậm chí hàng nghìn địa chỉ IP với một địa chỉ MAC duy nhất, có khả năng áp đảo máy mục tiêu. Loại tấn công này, đôi khi được gọi là ARP flooding, cũng có thể được sử dụng để nhắm mục tiêu vào switch, có khả năng ảnh hưởng đến hiệu suất của toàn bộ mạng.

1.2.4 Phương pháp phát hiện:

Dưới đây là một cách đơn giản để phát hiện bộ nhớ cache ARP của một thiết bị cụ thể đã bị nhiễm độc, bằng cách sử dụng command line. Khởi động trình hệ điều hành với tư cách quản trị viên. Sử dụng lệnh sau để hiển thị bảng ARP, trên cả Windows và Linux:

arp -n

Output giống như sau:

IP Address	MAC Address
192.168.5.1	00-14-22-01-23-45
192.168.5.201	40-d4-48-cr-55-b8
192.168.5.202	00-14-22-01-23-45

Nếu bảng chứa hai địa chỉ IP khác nhau có cùng địa chỉ MAC, chứng tỏ một cuộc tấn công ARP đang diễn ra. Vì địa chỉ IP 192.168.5.1 có thể được nhận dạng là bộ định tuyến nên IP của kẻ tấn công có thể là 192.168.5.202.

Để phát hiện ARP spoofing trong một mạng lớn và biết thêm thông tin về loại giao tiếp mà kẻ tấn công đang thực hiện, có thể sử dụng phần mềm Wireshark mã nguồn mở để bắt và phân tích gói tin.

Công cụ chống giả mạo XArp cũng sẽ giúp quá trình này dễ dàng hơn. Nó có thể cung cấp cảnh báo khi tấn công ARP bắt đầu, có nghĩa là các cuộc tấn công được phát hiện sớm hơn và thiệt hại có thể được giảm thiểu.

1.2.5 Biện pháp phòng chống:

Dưới đây là một số phương pháp tốt nhất có thể giúp ngăn chặn ARP Spoofing trên mạng của mình:

- Sử dụng Mạng riêng ảo (Virtual Private Network – VPN) cho phép các thiết bị kết nối với Internet thông qua một tunnel được mã hóa. Điều này làm cho tất cả thông tin liên lạc được mã hóa và vô giá trị đối với kẻ tấn công ARP spoofing.
- Sử dụng ARP tĩnh – giao thức ARP cho phép xác định mục nhập ARP tĩnh cho địa chỉ IP và ngăn thiết bị nghe phản hồi ARP cho địa chỉ đó. Ví dụ: nếu một máy tính luôn kết nối với cùng một bộ định tuyến, bạn có thể xác định một mục ARP tĩnh cho bộ định tuyến đó, điều này giúp ngăn chặn một cuộc tấn công.
- Sử dụng packet filtering – các packet filtering có thể xác định các gói ARP bị nhiễm độc bằng cách phát hiện chúng chứa thông tin nguồn xung đột và ngăn chúng lại trước khi chúng đến được các thiết bị trên mạng của bạn.
- Thực hiện một cuộc tấn công ARP spoofing – kiểm tra xem các hệ thống bảo mật hiện tại của bạn có đang hoạt động hay không bằng cách thực hiện một cuộc tấn công ARP spoofing với sự phối hợp của các nhóm Công nghệ thông tin và bảo mật. Nếu cuộc tấn công thành công, hãy xác định điểm yếu trong các biện pháp bảo mật của bạn và khắc phục chúng.

CHƯƠNG 2. THIẾT KẾ VÀ XÂY DỰNG CHƯƠNG TRÌNH

2.1 Giới thiệu chương trình:

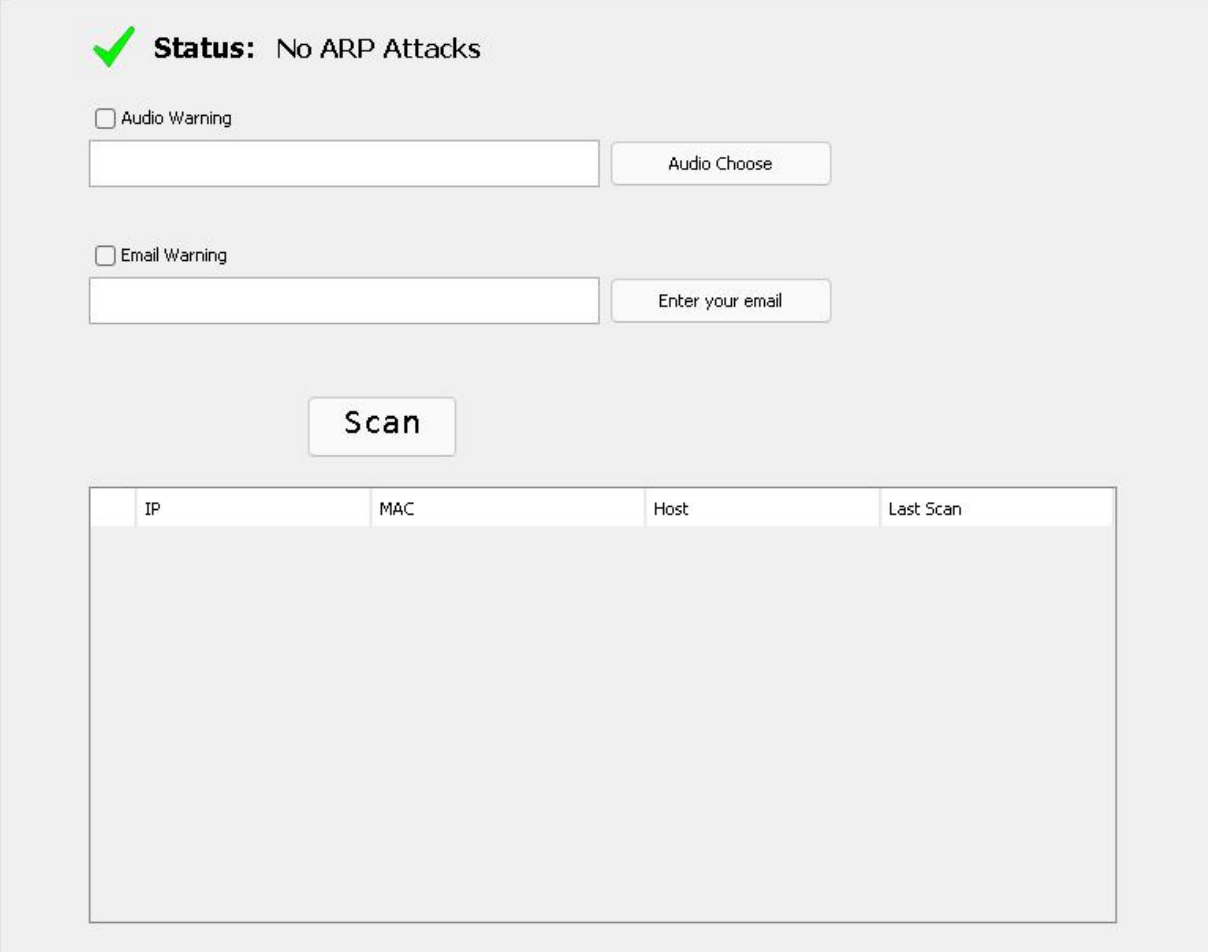
- PTITHCM_ARP_POLICE là chương trình giám sát bảng ARP trong máy tính, dựa trên sự thay đổi của các cặp IP và MAC trong bảng để đưa ra cảnh báo khi chương trình bị tấn công. Chương trình có các loại cảnh báo như cảnh báo bằng giao diện, cảnh báo qua email, phát âm thanh cảnh báo khi phát hiện bị tấn công và sẽ ghi logfile để từ đó người quản trị có thể phát hiện kịp thời để đưa ra các biện pháp khắc phục và phòng chống việc bị tấn công hệ thống.

2.2 Thực hiện:

2.2.1 Giải thuật phát hiện ARP Cache Poisoning:

- Dựa vào phương pháp phát hiện bằng cách sử dụng lệnh arp -a để kiểm tra trong bảng ARP có địa chỉ MAC nào lặp lại không. Nếu có thì kết luận phát hiện và cảnh báo qua âm thanh, qua giao diện, gửi mail và ghi log các thông tin cuộc tấn công

như địa chỉ IP, MAC address, thời gian... và thoát khỏi vòng lặp. Nếu hết vòng lặp mà không phát hiện thì thông báo không bị tấn công.



✓ **Status:** No ARP Attacks

☐ Audio Warning

Audio Choose

☐ Email Warning

Enter your email

Scan

IP	MAC	Host	Last Scan
----	-----	------	-----------

2.2.2 Cảnh báo trên giao diện:

- Khi phát hiện tấn công thì label “Status” sẽ hiện ra thông tin “ARP Poisoning detection” và các IP trên bị tấn công trên bảng sẽ được đánh dấu “X” nhận biết các host đang bị tấn công và hiển thị lên một hộp thoại thông báo và hộp thoại thông báo này chỉ tắt khi không bị tấn công nữa hoặc người dùng nhấn vào nút “I know it” trong hộp thoại thông báo.

2.2.3 Cảnh báo qua âm thanh:

- Khi scan và phát hiện tấn công thì ứng dụng sẽ phát âm thanh cảnh báo cho đến khi hết cuộc tấn công kết thúc hoặc được người dùng nhấn vào nút “I know it” trong hộp thoại thông báo.

2.2.4 Cảnh báo qua email:

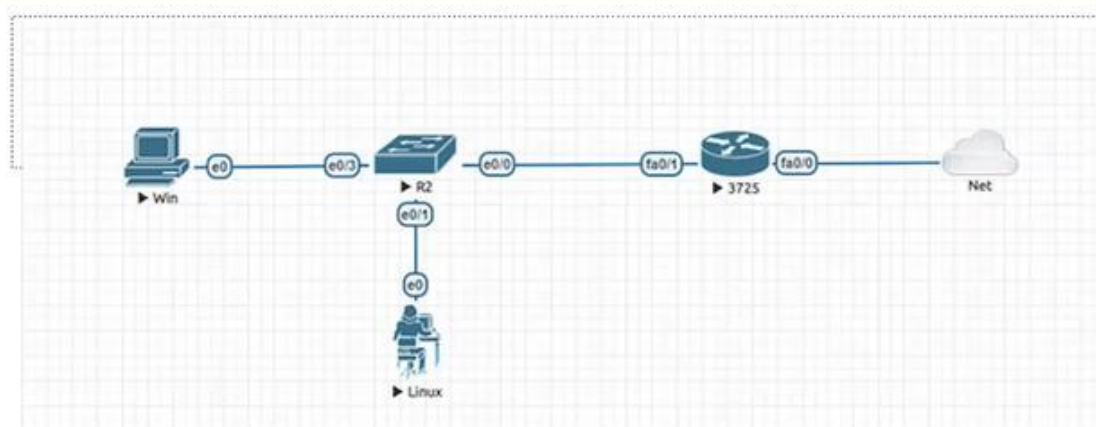
- Khi bị tấn công thì sẽ gửi đến email mà được nhập vào trên giao diện một thông báo hệ thống đã bị tấn công, các host bị tấn công và thời gian khi bị tấn công.

CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

3.1 Kịch bản 1: Sử dụng Ettercap trên máy Kali thực hiện ARP Poisoning và xem cấu hình thiết bị khi telnet của người dùng:

3.1.1 Tấn công:

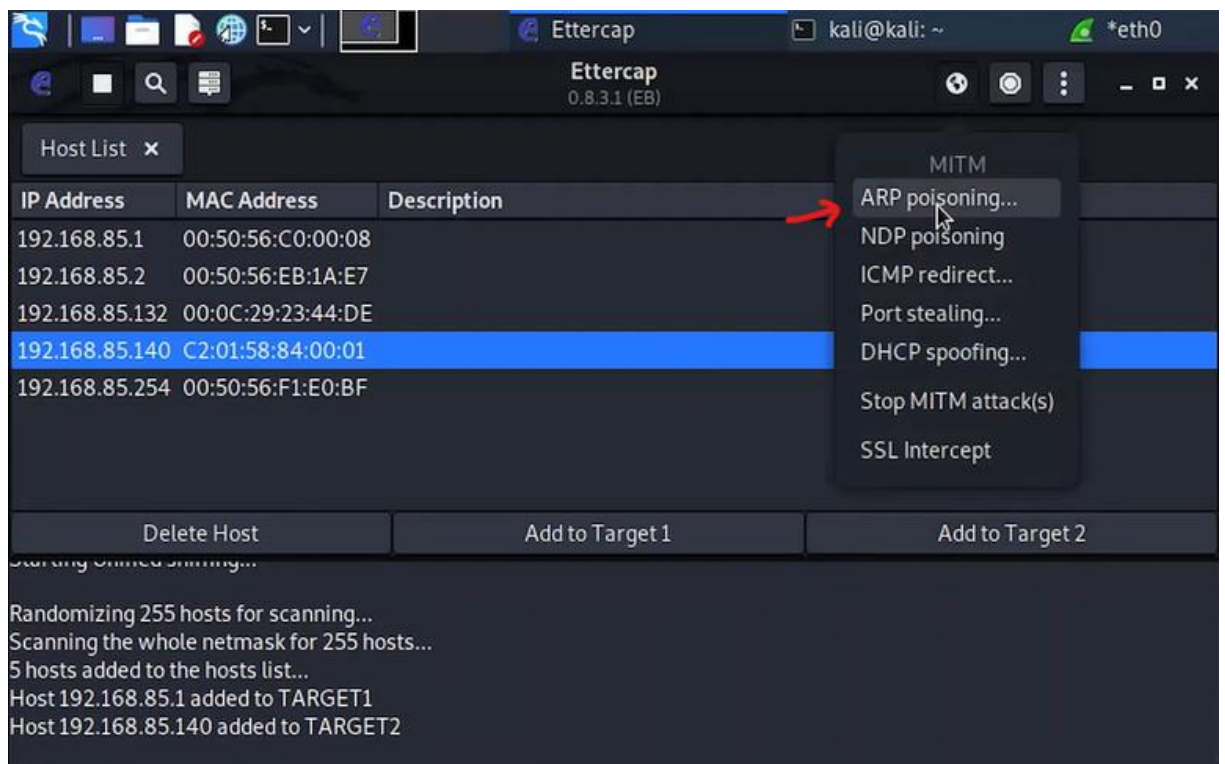
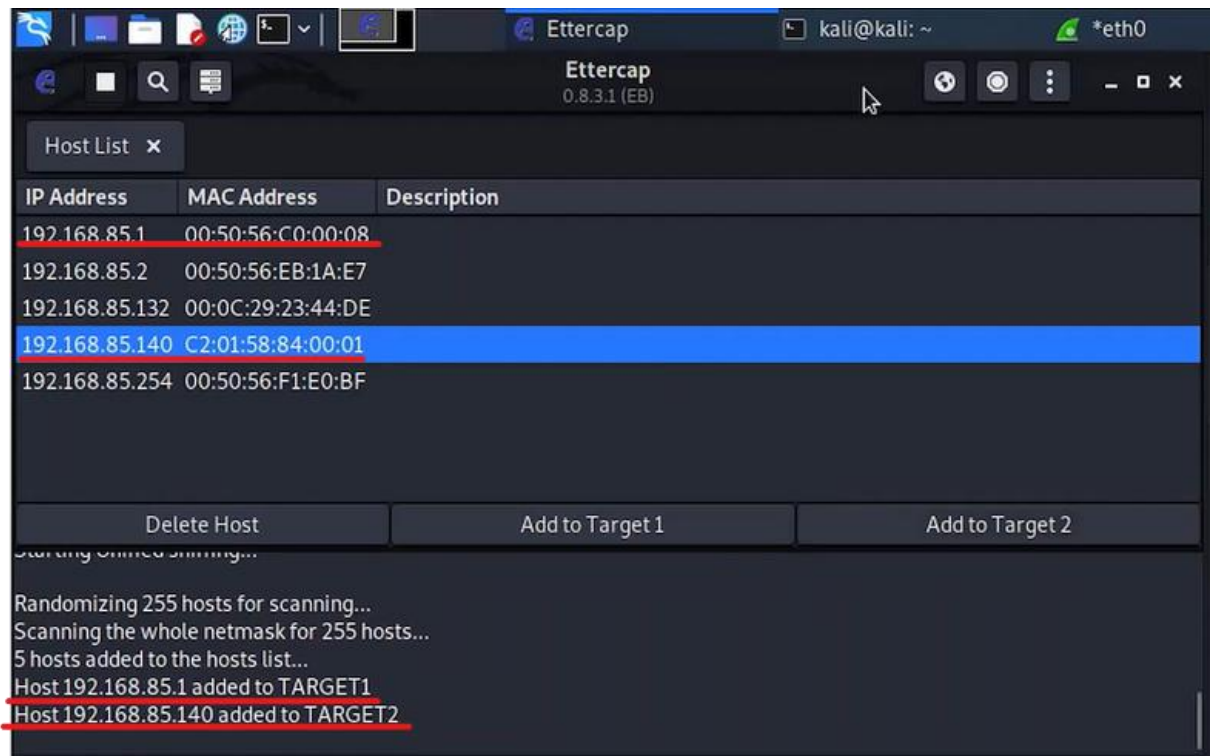
Bước 1: Truy cập vào mạng LAN nơi cần tấn công.



Thực hiện bắt gói tin khi máy Win telnet vào router:

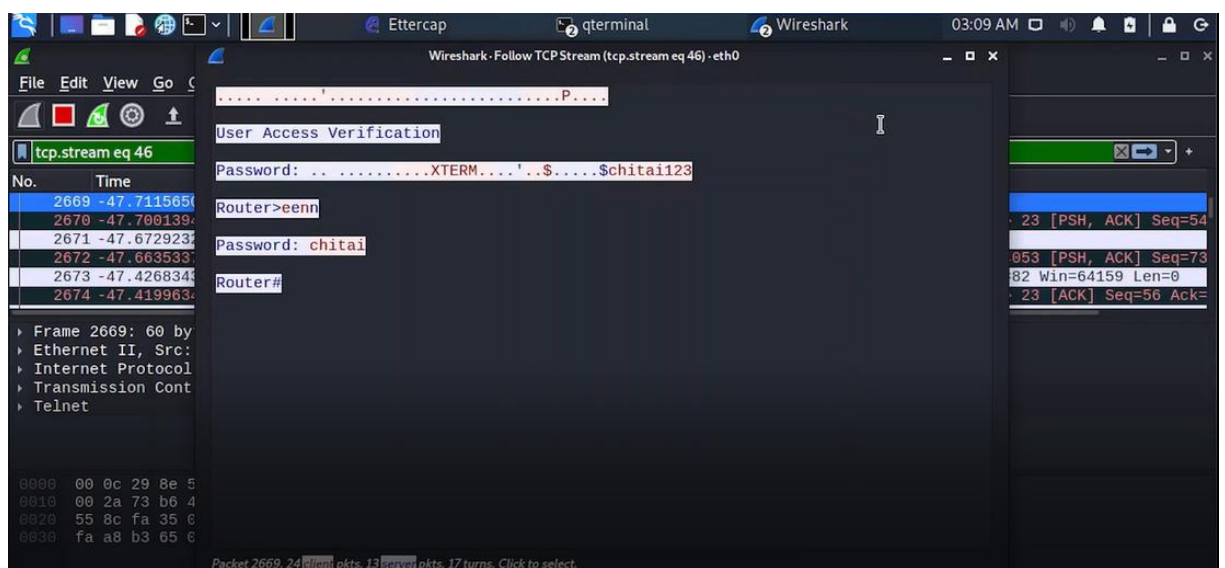
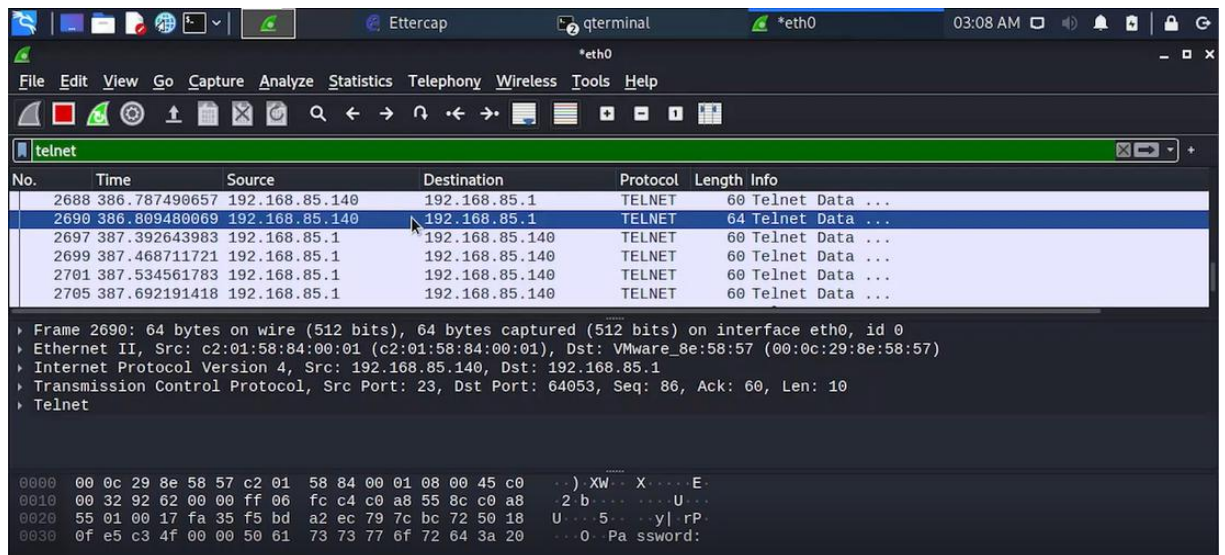
- + Sử dụng Ettercap thực hiện ARP poisoning.
- + Dùng Wireshark để xem gói tin.

Bước 2: Sử dụng Ettercap trên Linux Scan các host trong mạng và thêm vào các target để tấn công và thực hiện tấn công ARP Poisoning.



Bước 3: Sử dụng Wireshark để xem các gói tin được gửi đi từ nạn nhân đến các thiết bị.

- Khi người dùng telnet vào router để cấu hình thì ta bắt được mật khẩu và các cấu hình khi người dùng cấu hình.

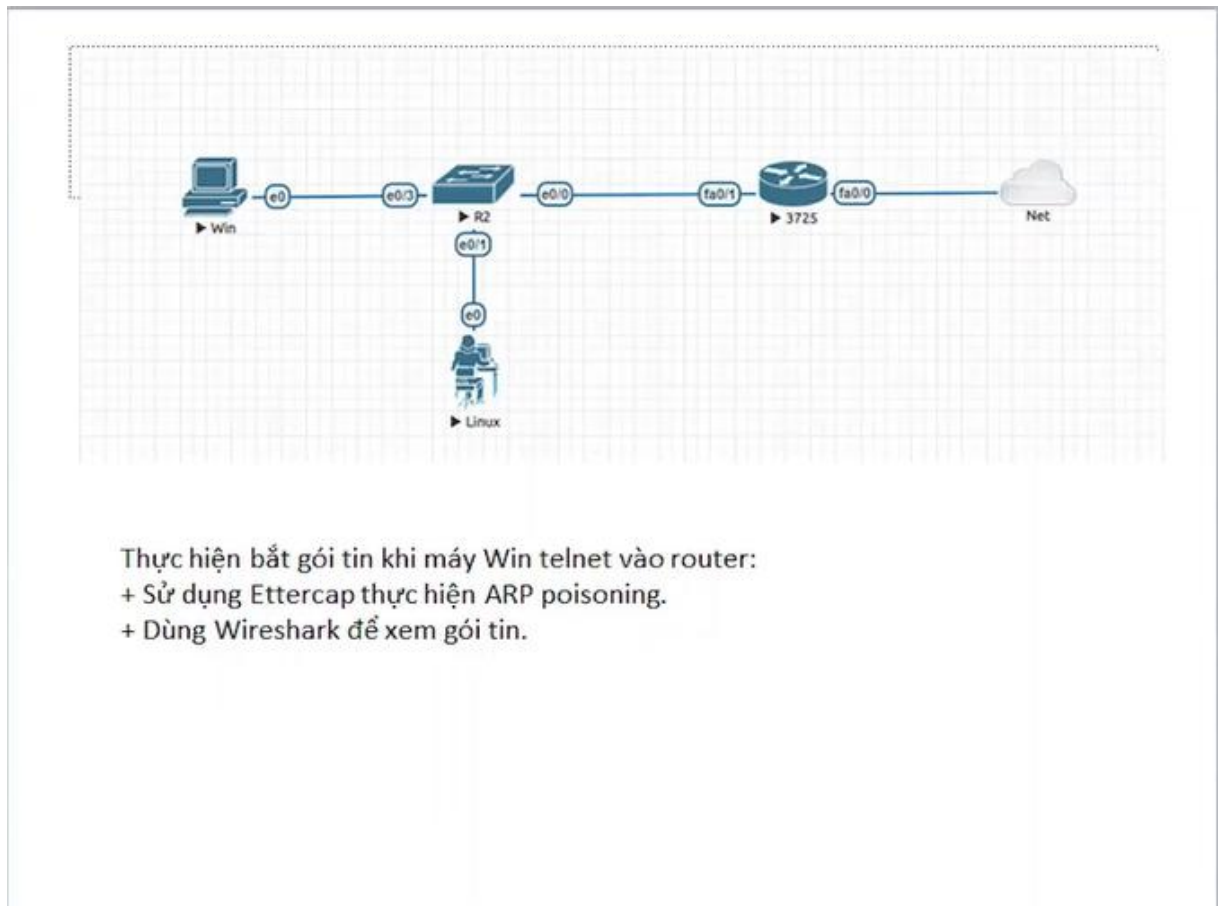
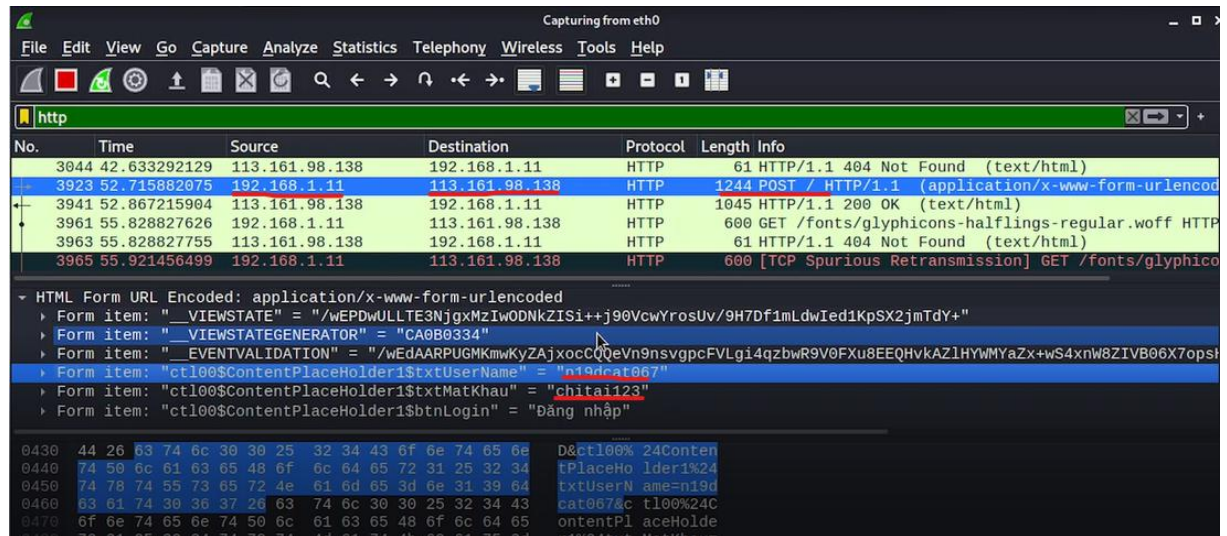


3.2 Kịch bản: Sử dụng Ettercap trên máy Kali thực hiện ARP Poisoning và thông tin của các gói tin(thông tin tài khoản và mật khẩu) khi người dùng truy cập các trang web sử dụng giao thức HTTP:

Trong phần này chúng em dự định trình bày về sử dụng Ettercap trên máy Kali thực hiện ARP Poisoning và sử dụng chương trình để phát hiện và cảnh báo thông qua các phương thức cảnh báo như trên giao diện, qua âm thanh và qua email.

3.2.1 Tấn công:

Bước 1: Truy cập vào LAN nơi cần tấn công.



Bước 2: Sử dụng Ettercap trên Linux Scan các host trong mạng và thêm vào các target để tấn công và thực hiện tấn công ARP Poisoning.

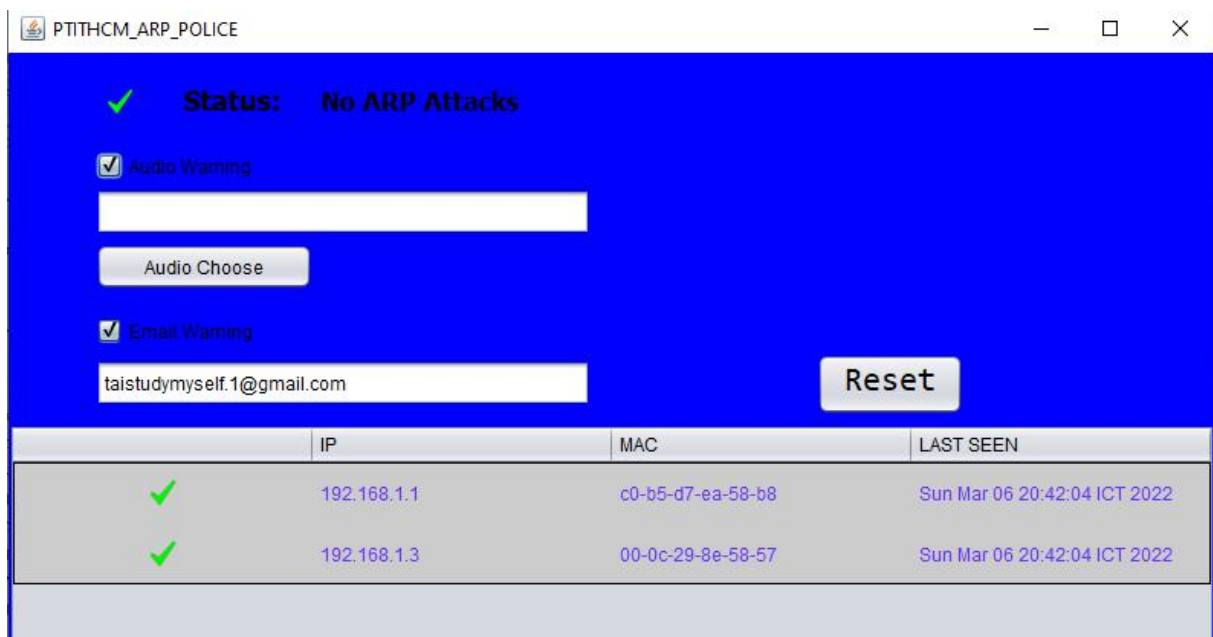
- Tương tự cách tấn công trên, chọn các host cần tấn công.

Bước 3: Sử dụng Wireshark để xem các gói tin giữa nạn nhân và trang web nạn nhân truy cập từ đó tìm thấy tài khoản đăng nhập và mật khẩu của người dùng.

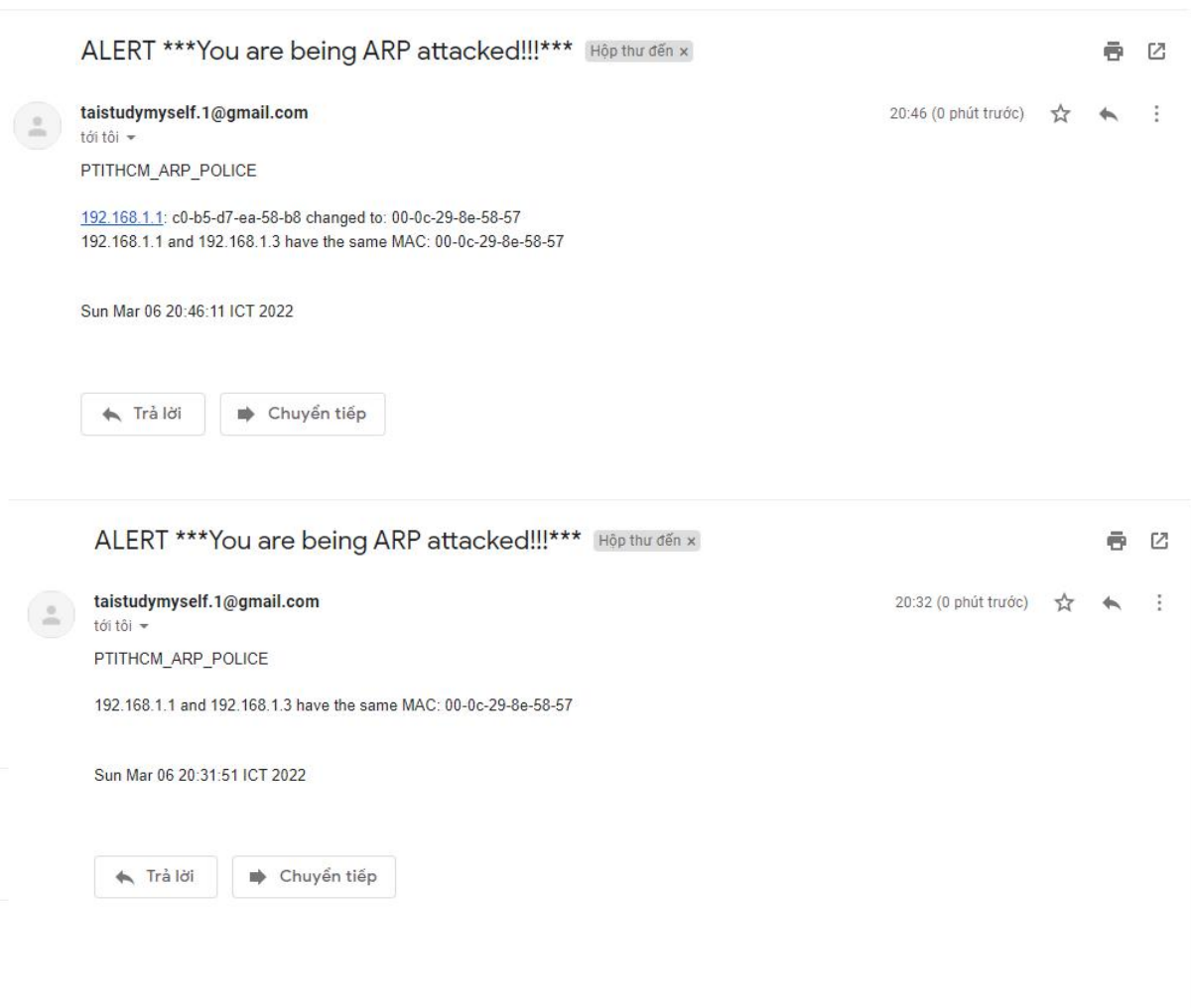
- Khi người dùng truy cập vào trang web ‘noibo.ptithcm.edu.vn’ và đăng nhập thì phương thức POST sẽ gửi các thông tin đăng nhập về trang web để xử lý đăng nhập lúc đó ta dùng Wireshark và tìm đến gói tin đấy và xem tài khoản đăng nhập và mật khẩu của người dùng.

3.3 Sử dụng chương trình để phát hiện tấn công:

- Khi chưa bị tấn công:



- Khi bị tấn công: thì chương trình sẽ thực hiện các hành động như thông báo trên giao diện, thông báo bằng phát một âm thanh cảnh báo và gửi email đến cho người dùng.



KẾT LUẬN

- Kết quả:

Chương trình hoàn thành đúng tiến độ và hiệu quả, thực hiện được các cảnh báo cần thiết cho người dùng khi phát hiện tấn công ARP Cache Poisoning để người dùng kịp đưa ra các phương án khắc phục và bảo vệ hệ thống của mình.

PTITHCM_ARP_POLICE được viết bằng ngôn ngữ Java và lập trình theo hướng đối tượng giúp việc nâng cấp sau này và triển khai trên nhiều hệ điều hành khác nhau dễ dàng và thuận tiện.

- Hạn chế:

Khi một máy trong mạng đổi card mạng thì vẫn thông báo là bị tấn công hoặc một số trường hợp đặc biệt khác. Dẫn đến vẫn có các thông báo giả, thiếu chính xác. Về phương thức gửi mail cảnh báo thì khi bị tấn công, nếu host có thể truy cập mạng thì có thể gửi truy cập đến server để gửi mail còn nếu thì gửi mail cảnh báo thất bại.

- Hướng phát triển:

Khắc phục hạn chế của phương thức gửi mail cảnh báo.

Áp dụng Machine Learning vào để ứng dụng nhạy cảm và chính xác hơn trong việc phát hiện tấn công.

TÀI LIỆU THAM KHẢO

- [1] David Kim, Michael G. Solomon, Fundamentals of information systems security(Third Edition), 2018.
- [2] Christopher A. Crayton, Ido Dubrawsky, Michael Cross, Jeremy Faircloth, Eli Faskha, Michael Gregg, Alun Jones, Marc Perez, Comptia Security+ Exam JKO-010 Study Guide and Practice Exam(Second Edition).
- [3] What is Address Resolution Protocol(ARP)?
<https://www.fortinet.com/resources/cyberglossary/what-is-arp>. Ngày 12/03/2022
- [4] Srinath Doss, “Detection and Prevention of ARP spoofing using Centralized Server”,International Journal of Computer Applications, March 2015
- [5] Jinhua, G. and Kejian, X. “ARP Spoofing detection algorithm using ICMP protocol”, IEEE Conference publication on Computer Communication and Informatics, pp.1-6, 2013.

TP. HCM, ngày 12 tháng 3 năm 2022
XÁC NHẬN CỦA GIẢNG VIÊN HƯỚNG DẪN

TS. Huỳnh Trọng Thừa Ths. Huỳnh Thanh Tâm