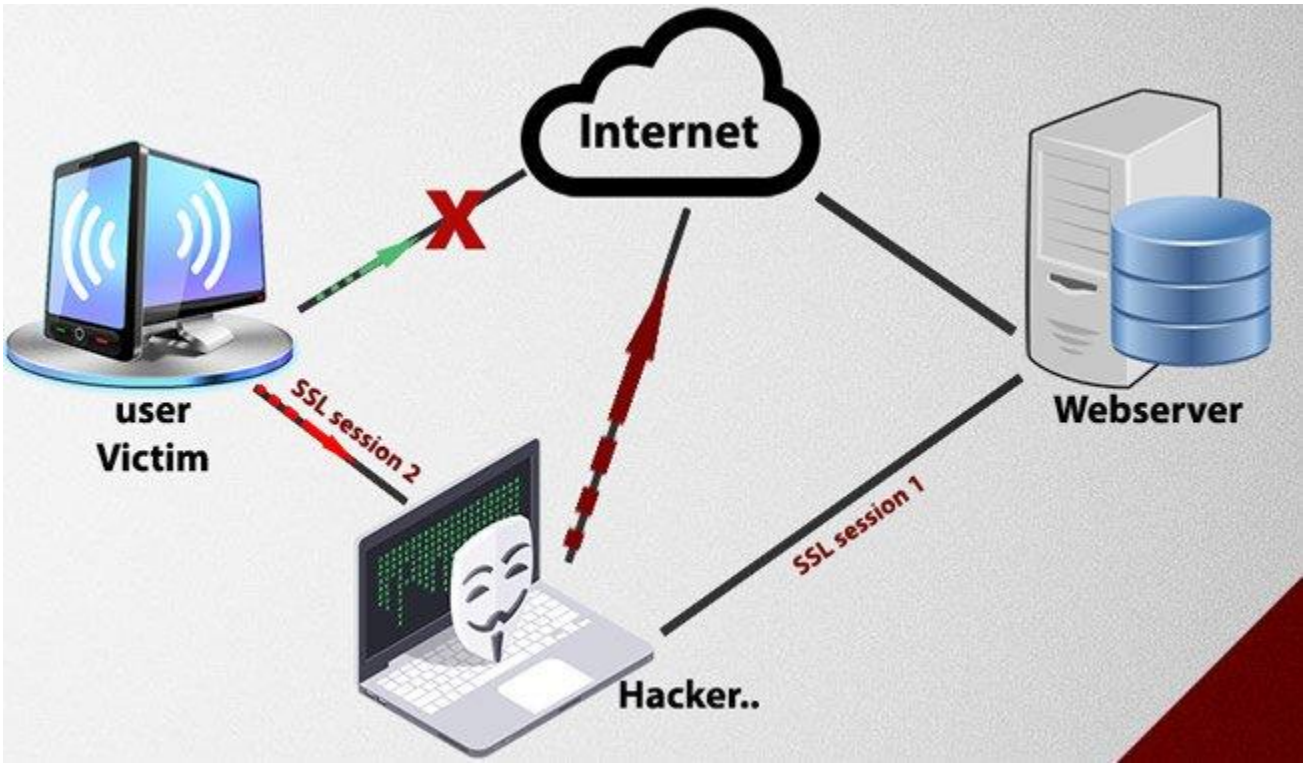
# Tìm hiểu về tấn công Man-in-the-Middle – Giả mạo ARP Cache

Trong phần đầu tiên của loạt bài giới thiệu về một số hình thức tấn công MITM hay được sử dụng nhất, chúng tôi sẽ giới thiệu cho các bạn về tấn công giả mạo ARP Cache, DNS Spoofing, chiếm quyền điều khiển (hijacking) HTTP session,..

**Man in the Middle là gì?**

Man in the Middle là một trong những kiểu tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính, nó thường được viết tắt là MITM. Có thể hiểu nôm na rằng MITM giống như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và chuyển tiếp dữ liệu giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, nhưng sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.




Trong loạt bài này, chúng tôi sẽ giải thích một số hình thức tấn công MITM hay được sử dụng nhất, chẳng hạn như tấn công giả mạo ARP Cache, DNS

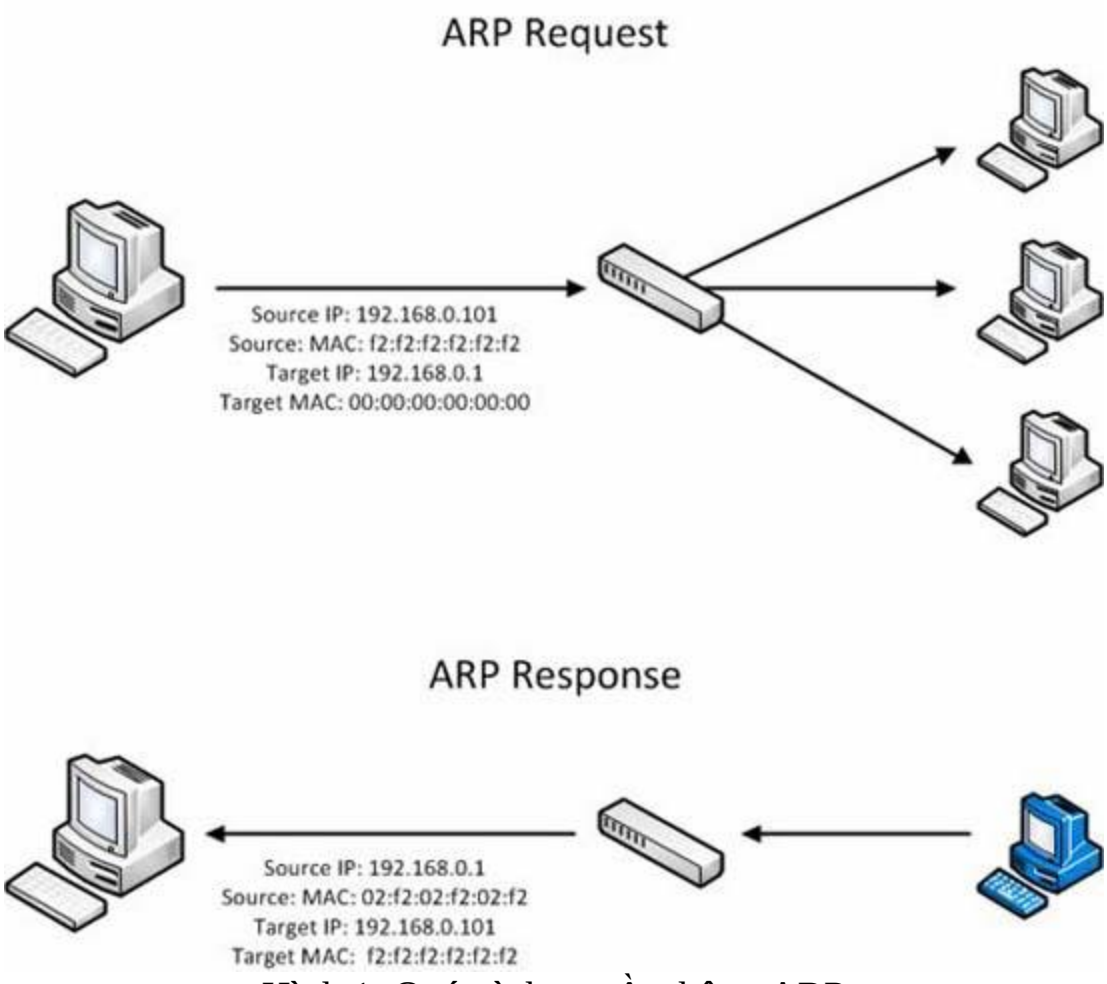
Spoofing, chiếm quyền điều khiển (hijacking) HTTP session,.. Như những gì bạn thấy trong thế giới thực, hầu hết các máy tính nạn nhân đều là các máy tính Windows. Với lý do đó, loạt bài này chúng tôi sẽ tập trung toàn bộ vào những khai thác MITM trên các máy tính đang chạy hệ điều hành Windows. Khi có thể, các cuộc tấn công MITM sẽ được thực hiện từ máy chủ chạy trên Windows. Tuy nhiên trong một số trường hợp, khi không có công cụ nào cho các tấn công được đề cập, chúng tôi sẽ sử dụng Backtrack Linux 4, có thể download dưới dạng một live-CD hoặc một máy ảo tại đây.

**Giả mạo ARP Cache (ARP Cache Poisoning)**

Trong phần đầu tiên của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn về việc giả mạo ARP cache. Đây là một hình thức tấn công MITM hiện đại có xuất xứ lâu đời nhất (đôi khi còn được biết đến với cái tên ARP Poison Routing), tấn công này cho phép hacker (nằm trên cùng một subnet với các nạn nhân của nó) có thể nghe trộm tất cả các lưu lượng mạng giữa các máy tính nạn nhân. Chúng tôi đã chọn đây là tấn công đầu tiên cần giới thiệu vì nó là một trong những hình thức tấn công đơn giản nhất nhưng lại là một hình thức hiệu quả nhất khi được thực hiện bởi kẻ tấn công.

**Truyền thông ARP thông thường**

Giao thức ARP được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa các lớp thứ hai và thứ ba trong mô hình OSI. Lớp thứ hai (lớp data-link) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp. Lớp thứ ba (lớp mạng), sử dụng địa chỉ IP để tạo các mạng có khả năng mở rộng trên toàn cầu. Lớp data-link xử lý trực tiếp với các thiết bị được kết nối với nhau, còn lớp mạng xử lý các thiết bị được kết nối trực tiếp và không trực tiếp. Mỗi lớp có cơ chế phân định địa chỉ riêng, và chúng phải làm việc với nhau để tạo nên một mạng truyền thông. Với lý do đó, ARP được tạo với RFC 826, "*một giao thức phân định địa chỉ Ethernet - Ethernet Address Resolution Protocol*".

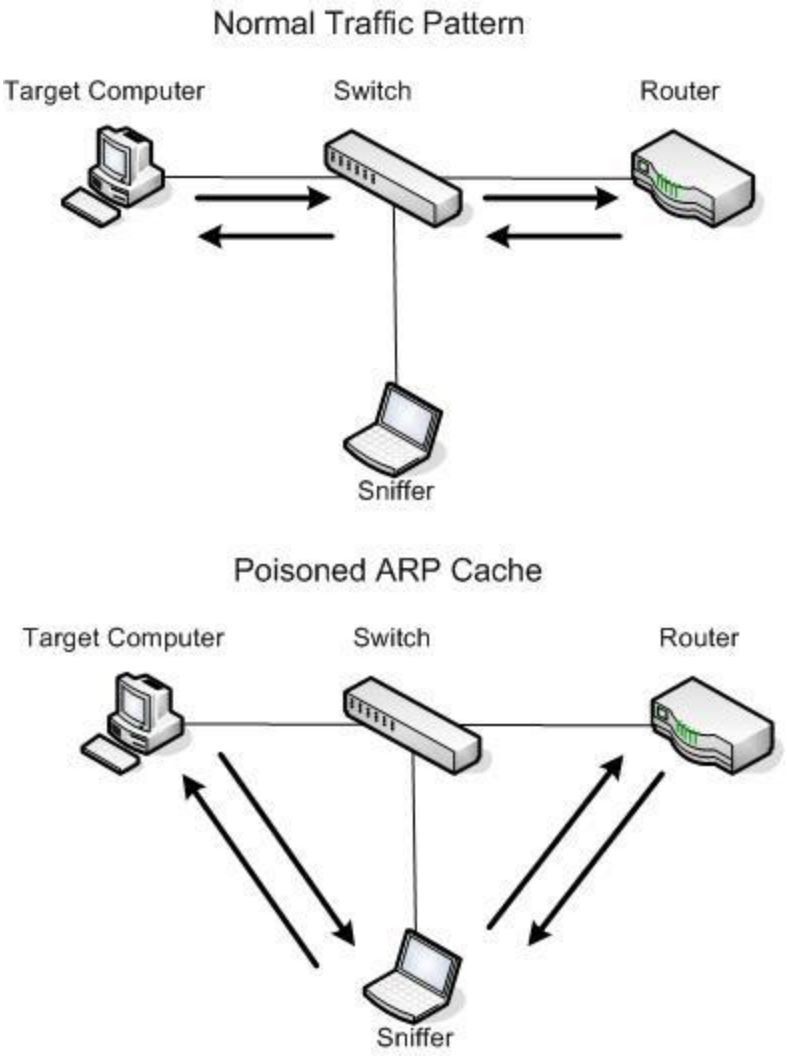



Hình 1: Quá trình truyền thông ARP

Thực chất trong vấn đề hoạt động của ARP được tập trung vào hai gói, một gói ARP request và một gói ARP reply. Mục đích của request và reply là tìm ra địa chỉ MAC phần cứng có liên quan tới địa chỉ IP đã cho để lưu lượng có thể đến được đích của nó trong mạng. Gói request được gửi đến các thiết bị trong đoạn mạng, trong khi gửi nó nói rằng (đây chỉ là nhân cách hóa để giải thích theo hướng dễ hiểu nhất) "*Hey, địa chỉ IP của tôi là XX.XX.XX.XX, địa chỉ MAC của tôi là XX:XX:XX:XX:XX:XX. Tôi cần gửi một vài thứ đến một người có địa chỉ XX.XX.XX.XX, nhưng tôi không biết địa chỉ phần cứng này nằm ở đâu trong đoạn mạng của mình. Nếu ai đó có địa chỉ IP này, xin hãy đáp trả lại kèm với địa chỉ MAC của mình!*" Đáp trả sẽ được gửi đi trong gói ARP reply và cung cấp câu trả lời, "*Hey thiết bị phát. Tôi là người mà bạn đang tìm kiếm với địa chỉ IP là XX.XX.XX.XX. Địa chỉ MAC của tôi là XX:XX:XX:XX:XX:XX.*" Khi quá trình này hoàn tất, thiết bị phát sẽ cập nhật bảng ARP cache của nó và hai thiết bị này có thể truyền thông với nhau.

**Việc giả mạo Cache**

Việc giả mạo bảng ARP chính là lợi dụng bản tính không an toàn của giao thức ARP. Không giống như các giao thức khác, chẳng hạn như DNS (có thể được cấu hình để chỉ chấp nhận các nâng cấp động khá an toàn), các thiết bị sử dụng giao thức phân giải địa chỉ (ARP) sẽ chấp nhận nâng cấp bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào có thể gửi gói ARP reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP cache của nó ngay giá trị mới này. Việc gửi một gói ARP reply khi không có request nào được tạo ra được gọi là việc gửi ARP "vu vơ". Khi các ARP reply vu vơ này đến được các máy tính đã gửi request, máy tính request này sẽ nghĩ rằng đó chính là đối tượng mình đang tìm kiếm để truyền thông, tuy nhiên thực chất họ lại đang truyền thông với một kẻ tấn công.



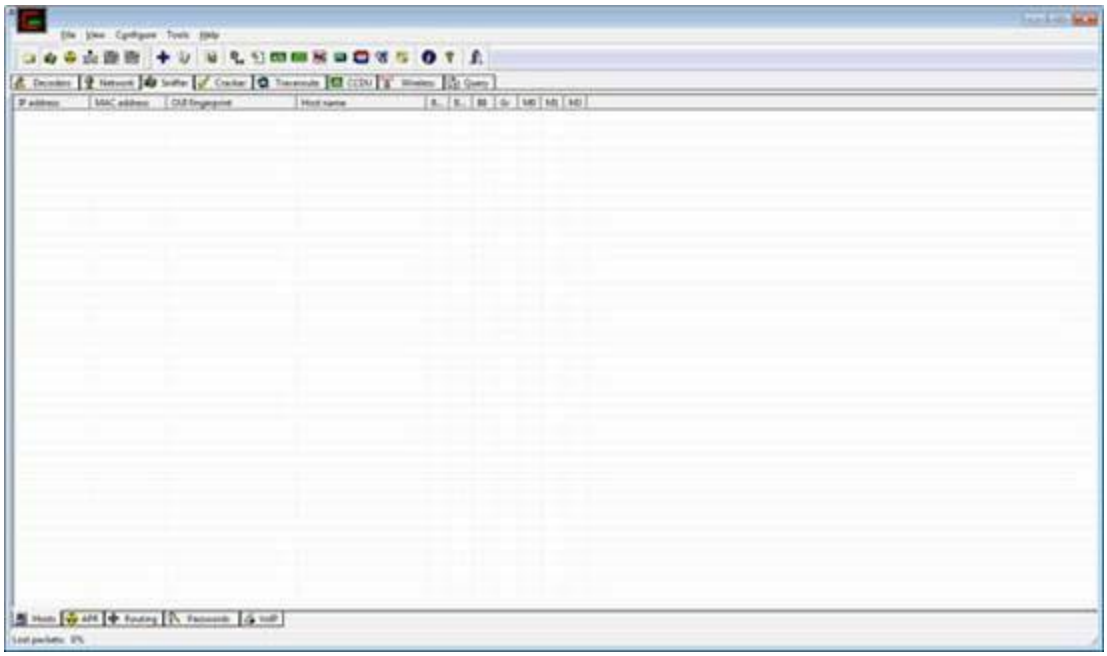
Hình 2: Chặn truyền thông bằng các giả mạo ARP Cache

**Sử dụng Cain & Abel**

Hãy để chúng tôi đưa ra một kịch bản và xem xét nó từ góc độ lý thuyết đến thực tế. Có một vài công cụ có thể thực hiện các bước cần thiết để giả mạo ARP cache của các máy tính nạn nhân. Chúng tôi sẽ sử dụng công cụ bảo mật khá phổ biến mang tên Cain & Abel của Oxid.it. Cain & Abel thực hiện khá nhiều thứ ngoài vấn đề giả mạo ARP cache, nó là một công cụ rất hữu dụng cần có trong kho vũ khí của bạn. Việc cài đặt công cụ này khá đơn giản.

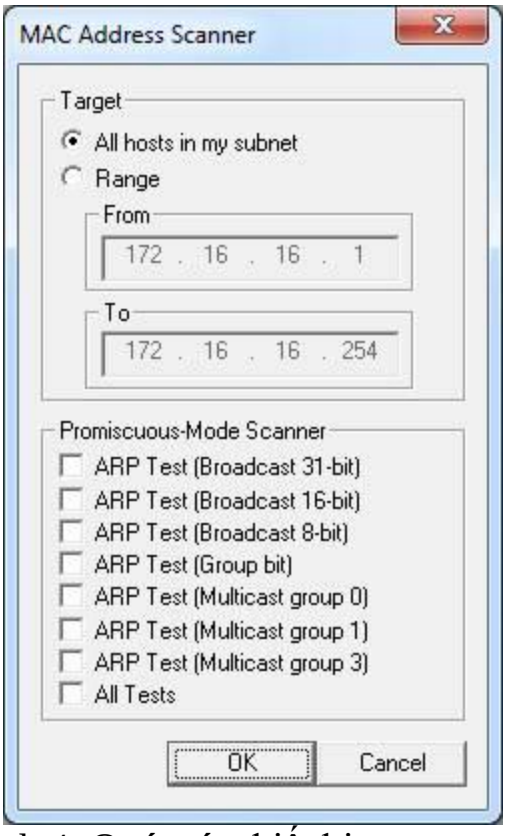
Trước khi bắt đầu, bạn cần lựa chọn một số thông tin bổ sung. Cụ thể như giao diện mạng muốn sử dụng cho tấn công, hai địa chỉ IP của máy tính nạn nhân.

Khi lần đầu mở Cain & Abel, bạn sẽ thấy một loạt các tab ở phía trên cửa sổ. Với mục đích của bài, chúng tôi sẽ làm việc trong tab Sniffer. Khi kích vào tab này, bạn sẽ thấy một bảng trống. Để điền vào bảng này bạn cần kích hoạt bộ sniffer đi kèm của chương trình và quét các máy tính trong mạng của bạn.



Hình 3: Tab Sniffer của Cain & Abel

Kích vào biểu tượng thứ hai trên thanh công cụ, giống như một card mạng. Thời gian đầu thực hiện, bạn sẽ bị yêu cầu chọn giao diện mà mình muốn sniff (đánh hơi). Giao diện cần phải được kết nối với mạng mà bạn sẽ thực hiện giả mạo ARP cache của mình trên đó. Khi đã chọn xong giao diện, kích **OK** để kích hoạt bộ sniffer đi kèm của Cain & Abel. Tại đây, biểu tượng thanh công cụ giống như card mạng sẽ bị nhấn xuống. Nếu không, bạn hãy thực hiện điều đó. Để xây dựng một danh sách các máy tính hiện có trong mạng của bạn, hãy kích biểu tượng giống như ký hiệu (+) trên thanh công cụ chính và kích **OK**.



Hình 4: Quét các thiết bị trong mạng

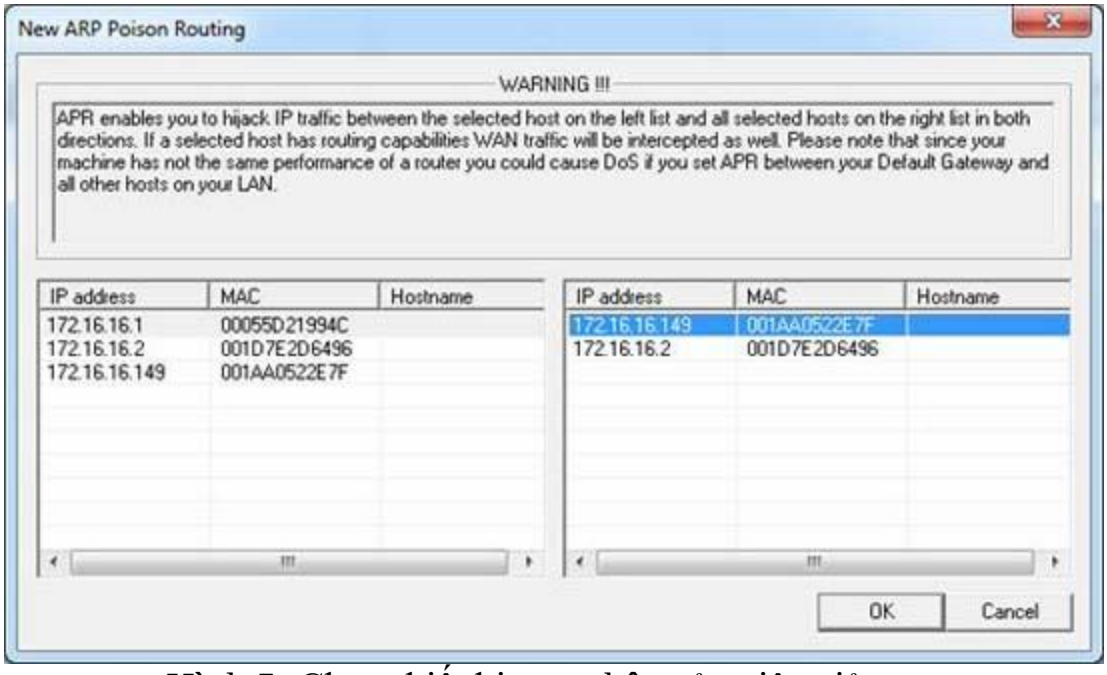
Những khung lưới trống rỗng lúc này sẽ được điền đầy bởi một danh sách tất cả các thiết bị trong mạng của bạn, cùng với đó là địa chỉ MAC, IP cũng như các thông tin nhận dạng của chúng. Đây là danh sách bạn sẽ làm việc khi thiết lập giả mạo ARP cache.

Ở phía dưới cửa sổ chương trình, bạn sẽ thấy một loạt các tab đưa bạn đến các cửa sổ khác bên dưới tiêu đề Sniffer. Lúc này bạn đã xây dựng được danh sách các thiết bị của mình, nhiệm vụ tiếp theo của bạn là làm việc với tab APR. Chuyển sang cửa sổ APR bằng cách kích tab.

Khi ở trong cửa sổ APR, bạn sẽ thấy hai bảng trống rỗng: một bên phía trên và một phía dưới. Khi thiết lập chúng, bảng phía trên sẽ hiển thị các thiết bị có liên quan trong giả mạo ARP cache và bảng bên dưới sẽ hiển thị tất cả truyền thông giữa các máy tính bị giả mạo.

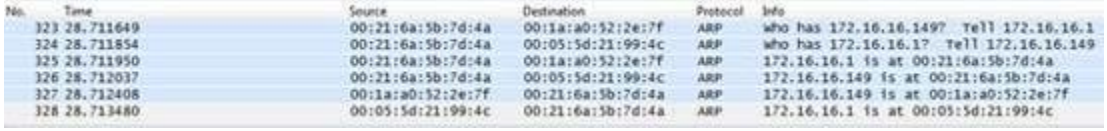
Tiếp tục thiết lập sự giả mạo ARP bằng cách kích vào biểu tượng giống như dấu (+) trên thanh công cụ chuẩn của chương trình. Cửa sổ xuất hiện có hai cột đặt cạnh nhau. Phía bên trái, bạn sẽ thấy một danh sách tất cả các thiết bị có sẵn trong mạng. Kích địa chỉ IP của một trong những nạn nhân, bạn sẽ thấy các kết quả hiện ra trong cửa sổ bên phải là danh sách tất cả các host

trong mạng, bỏ qua địa chỉ IP vừa chọn. Trong cửa sổ bên phải, kích vào địa chỉ IP của nạn nhân khác và kích **OK**.




Hình 5: Chọn thiết bị nạn nhân của việc giả mạo

Các địa chỉ IP của cả hai thiết bị lúc này sẽ được liệt kê trong bảng phía trên của cửa sổ ứng dụng chính. Để hoàn tất quá trình, kích vào ký hiệu bức xạ (vàng đen) trên thanh công cụ chuẩn. Điều đó sẽ kích hoạt các tính năng giả mạo ARP cache của Cain & Abel và cho phép hệ thống phân tích của bạn trở thành người nghe lén tất cả các cuột truyền thông giữa hai nạn nhân. Nếu bạn muốn thấy những gì đang diễn ra sau phông này, hãy cài đặt Wireshark và lắng nghe từ giao diện khi bạn kích hoạt giả mạo. Bạn sẽ thấy lưu lượng ARP đến hai thiết bị và ngay lập tức thấy sự truyền thông giữa chúng.




Hình 6: Chèn lưu lượng ARP

Khi kết thúc, hãy kích vào ký hiệu bức xạ (vàng đen) lần nữa để ngừng hành động giả mạo ARP cache.

## Biện pháp phòng chống

Nghiên cứu quá trình giả mạo ARP cache từ quan điểm của người phòng chống, chúng ta có một chút bất lợi. Quá trình ARP xảy ra trong chế độ background nên có rất ít khả năng có thể điều khiển trực tiếp được chúng. Không có một giải pháp cụ thể nào, tuy nhiên chúng ta vẫn cần những lập

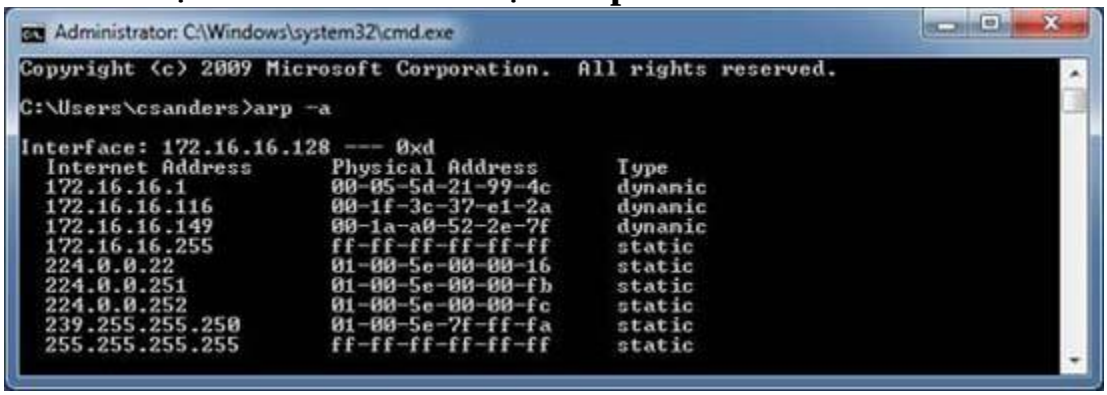
trường đi tiên phong và phản ứng trở lại nếu bạn lo lắng đến vấn đề giả mạo ARP cache trong mạng của mình.

**Bảo mật LAN**

Giả mạo ARP Cache chỉ là một kỹ thuật tấn công mà nó chỉ sống sót khi cố gắng chặn lưu lượng giữa hai thiết bị trên cùng một LAN. Chỉ có một lý do khiến cho bạn lo sợ về vấn đề này là liệu thiết bị nội bộ trên mạng của bạn có bị thỏa hiệp, người dùng tin cậy có ý định hiểm độc hay không hoặc liệu có ai đó có thể cắm một thiết bị không tin cậy vào mạng. Mặc dù chúng ta thường tập trung toàn bộ những cố gắng bảo mật của mình lên phạm vi mạng nhưng việc phòng chống lại những mối đe dọa ngay từ bên trong và việc có một thái độ bảo mật bên trong tốt có thể giúp bạn loại trừ được sự sợ hãi trong tấn công được đề cập ở đây.

**Mã hóa ARP Cache**

Một cách có thể bảo vệ chống lại vấn đề không an toàn vốn có trong các ARP request và ARP reply là thực hiện một quá trình kém động hơn. Đây là một tùy chọn vì các máy tính Windows cho phép bạn có thể bổ sung các entry tĩnh vào ARP cache. Bạn có thể xem ARP cache của máy tính Windows bằng cách mở nhắc lệnh và đánh vào đó lệnh **arp –a**.




Hình 7: Xem ARP Cache

Có thể thêm các entry vào danh sách này bằng cách sử dụng lệnh **arp –s <IP ADDRESS> <MAC ADDRESS>**.

Trong các trường hợp, nơi cấu hình mạng của bạn không mấy khi thay đổi, bạn hoàn toàn có thể tạo một danh sách các entry ARP tĩnh và sử dụng chúng cho các client thông qua một kịch bản tự động. Điều này sẽ bảo đảm được các thiết bị sẽ luôn dựa vào ARP cache nội bộ của chúng thay vì các ARP request và ARP reply.

**Kiểm tra lưu lượng ARP với chương trình của hãng thứ ba**

Tùy chọn cuối cùng cho việc phòng chống lại hiện tượng giả mạo ARP cache là phương pháp phản ứng có liên quan đến việc kiểm tra lưu lượng mạng của các thiết bị. Bạn có thể thực hiện điều này với một vài hệ thống phát hiện xâm phạm (chẳng hạn như Snort) hoặc thông qua các tiện ích được thiết kế đặc biệt cho mục đích này (như xARP). Điều này có thể khả thi khi bạn chỉ quan tâm đến một thiết bị nào đó, tuy nhiên nó vẫn khá cồng kềnh và vướng mắc trong việc giải quyết với toàn bộ đoạn mạng.

**Kết luận**

Giả mạo ARP Cache là một chiêu khá hiệu quả trong thế giới những kẻ tấn công thụ động "man-in-the-middle" vì nó rất đơn giản nhưng lại hiệu quả. Hiện việc giả mạo ARP Cache vẫn là một mối đe dọa rất thực trên các mạng hiện đại, vừa khó bị phát hiện và khó đánh trả. Trong phần tiếp theo của loạt bài này, chúng tôi sẽ tập trung vào vấn đề phân giải tên và khái niệm giả mạo DNS.

***ARP và nguyên tắc làm việc trong mạng LAN***

Như ta đã biết tại tầng Network của mô hình OSI , chúng ta thường sử dụng các loại địa chỉ mang tính chất quy ước như IP, IPX… Các địa chỉ này được phân thành hai phần riêng biệt là phần địa chỉ mạng (NetID) và phần địa chỉ máy ( HostID) . Cách đánh số địa chỉ như vậy nhằm giúp cho việc tìm ra các đường kết nối từ hệ thống mạng này sang hệ thống mạng khác được dễ dàng hơn. Các địa chỉ này có thể được thay đổi theo tùy ý người sử dụng.

Trên thực tế, các card mạng (NIC) chỉ có thể kết nối với nhau theo địa chỉ MAC, địa chỉ cố định và duy nhất của phần cứng. Do vậy ta phải có một cơ chế để chuyển đổi các dạng địa chỉ này qua lại với nhau. Từ đó ta có giao thức phân giải địa chỉ: Address Resolution Protocol (ARP).

***Nguyên tắc làm việc của ARP trong một mạng LAN***

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong

request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản, ví dụ như PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của PC có địa chỉ IP này là gì ?" Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, PC B sẽ gửi lại một gói tin cho PC A trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.

***Nguyên tắc hoạt động của ARP trong môi trường hệ thống mạng***

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau :

- Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.

- Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.

- Máy A truyền gói tin đến port X của Router.

- Router nhận được gói tin từ máy A, chuyển gói tin ra port Y của

Router. Trong gói tin có chứa địa chỉ IP của máy B. Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.

- Máy B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của máy B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy.

***ARP cache***

ARP cache có thể coi như một bảng có chứa một tập tương ứng giữa các phần cứng và địa chỉ Internet Protocol (IP). Mỗi một thiết bị trên một mạng nào đó đều có cache riêng. Có hai cách lưu giữ các entry trong cache để phân giải địa chỉ diễn ra nhanh. Đó là:

* Các entry ARP Cache tĩnh. Ở đây, sự phân giải địa chỉ phải được *add* một cách thủ công vào bảng cache và được duy trì lâu dài.

* Các entry ARP Cache động. Ở đây, các địa chỉ IP và phần cứng được giữ trong cache bởi phần mềm sau khi nhận được kết quả của việc hoàn thành quá trình phân giải trước đó. Các địa chỉ được giữ tạm thời và sau đó được gỡ bỏ.

ARP Cache biến một quá trình có thể gây lãng phí về mặt thời gian thành một quá trình sử dụng thời gian một cách hiệu quả. Mặc dù vậy nó có thể bắt gặp một số vấn đề. Cần phải duy trì bảng cache. Thêm vào đó cũng có thể các entry cache bị "cũ" theo thời gian, vì vậy cần phải thực thi hết hiệu lực đối với các entry cache sau một quãng thời gian nào đó.