Bài: 8.1 Nghe trộm - Khái niệm nghe trộm, tấn công MAC, DHCP.

Xem bài học trên website để ủng hộ Kteam: 8.1 Nghe trộm - Khái niệm nghe trộm, tấn công MAC, DHCP.

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tóm tắt

Ở chương này chúng ta sẽ tìm hiểu **việc nghe trộm**. Nghe trộm giúp chúng ta quan sát tất cả các loại giao thông mạng, dù mạng được bảo vệ hay không. Những thông tin nghe trộm được có thể hữu ích cho tấn công và tạo trở ngại cho nạn nhân. Bên cạnh đó, chúng ta sẽ tìm hiểu nhiều loại tấn công như **Media Access Control** (**MAC**), **Dynamic Host Configuration Protocol** (**DHCP**), **Address Resolution Protocol** (**ARP**) **Poisoning**, **MAC Spoofing**, **DNS Poisoning**.

Sau khi nghe trộm xong, bạn có thể tiếp tục thực hiện các loại tấn công như **Session Hijacking**, **DoS Attacks**, **MITM attack,** ... Tuy nhiên hãy nhớ rằng công cụ nghe trộm không phải công cụ hacking. Chúng là những công cụ chẩn đoán, thường dùng để quan sát mạng và những vấn đề xử lí sự cố.

Khái niệm nghe trộm

Giới thiệu sơ lược về nghe trộm

Nghe trộm là quá trình sử dụng công cụ để quét và quan sát những gói tin truyền trong hệ thống. Quy trình nghe trộm được thực hiện bằng port hỗn tạp. Kích hoạt **trạng thái hỗn tạp** sẽ giúp thu thập được mọi loại giao thông. Một khi đã thu thập được gói tin, kẻ tấn công dễ dàng thăm dò nội dung bên trong.

Có hai loại nghe trộm:

1. Nghe trộm chủ động
2. Nghe trộm thụ động

Kẻ tấn công có thể thu thập được các loại gói tin như **Syslog**, **DNS**, **Web**, **email** và **các loại dữ liệu khác** truyền qua hệ thống mạng nhờ nghe trộm. Thu thập gói tin giúp kẻ tấn công lấy được các thông tin như dữ liệu, tên người dùng, mật khẩu từ những giao thức như **HTTP**, **POP**, **IMAP**, **SMTP**, **NMTP**, **FTP**, **Telnet**, và **Rlogin** cũng như nhiều thông tin khác. Những người ở trong mạng LAN hoặc kết nối với cùng một mạng có thể nghe trộm gói tin. Tiếp theo chúng ta tập trung nghiên cứu cách thức kẻ nghe trộm thực hiện hành động cũng như những thứ nghe trộm có thể lấy cắp.

Cách thức hoạt động của kẻ nghe trộm

Đầu tiên, kẻ tấn công sẽ kết nối với một hệ thống mạng để nghe trộm. Kẻ tấn công sử dụng **công cụ sniffer** để kích hoạt trạng thái hỗn tạp trong thẻ giao diện hệ thống (NIC) của hệ thống nạn nhân, từ đó thu thập gói tin. Trong trạng thái hỗn tạp, NIC phản hồi với mọi gói tin nó nhận được. Như bạn thấy ở hình dưới, kẻ tấn công được kết nối trong trạng thái hỗn tạp và chấp nhận gói tin dù gói tin đó không được gửi cho hắn.

Sau khi thu thập, kẻ tấn công có thể giải hóa gói tin để trích rút thông tin. Nguyên tắc cơ bản đằng sau kĩ thuật này là

- Bạn kết nối được với một hệ thống mục tiêu có **switch** (trái với **hub** và **broadcast**) và giao thông **multicast** truyền trên mọi cổng.
- **Switch** chuyển tiếp gói tin **unicast** đến port riêng kết nối với host thật.
- Switch duy trì bảng MAC để xác nhận người nào đang kết nối với port nào.

Trong trường hợp này, kẻ tấn công thay đổi thiết lập switch bằng nhiều kĩ thuật khác nhau như **Port Mirroring** hoặc **Switched Port Analyzer** (SPAN). Tất cả các gói tin truyền qua một port nhất định sẽ được sao chép trên port đó (kẻ tấn công kết nối với port này trong trạng thái hỗn tạp). Nếu bạn kết nối với hub, nó sẽ truyền gói tin đến tất cả các port.

Copyright © Howkteam.com

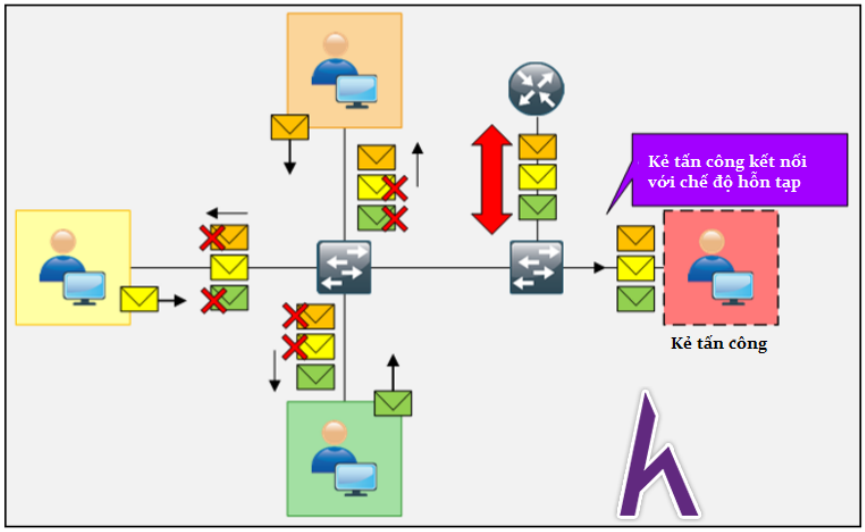


Figure 8-01 Packet Sniffing

Các loại nghe trộm

Nghe trộm thụ động

Đây là loại nghe trộm không cần gửi thêm gói tin hoặc can thiệp vào các thiết bị như hub để nhận gói tin. Như chúng ta đã biết, hub truyền gói tin đến port của nó. Kẻ tấn công có thể lợi dụng điểm này để dễ dàng quan sát giao thông truyền qua mạng.

Nghe trộm chủ động

Đây là loại nghe trộm mà kẻ tấn công cần gửi thêm gói tin đến thiết bị đã kết nối như switch để nhận gói tin. Như đã nói, switch chỉ truyền gói tin unicast đến một port nhất định. Kẻ tấn công sử dụng một số kĩ thuật như **MAC Flooding**, **DHCP Attacks**, **DNS poisoning**, **Switch Port Stealing**, **ARP Poisoning**, và **Spoofing** để quan sát giao thông truyền qua switch. Những kĩ thuật này sẽ được giới thiệu ở phần sau của chương.

Công cụ phân tích giao thức phần cứng

Máy phân tích giao thức phần cứng hay phần mềm đều dùng để phân tích gói tin và tín hiệu truyền qua kênh truyền dẫn. Máy phân tích giao thức phần cứng là những thiết bị thu thập gói tin mà không can thiệp vào giao thông mạng. Một ưu điểm lớn của thiết bị này là sự lưu động, linh hoạt, và lưu tốc. Kẻ tấn công có thể sử dụng máy phân tích giao thức này để:

- Quan sát network usage
- Nhận diện giao thông từ phần mềm hacking
- Giải hóa gói tin
- Trích rút thông tin
- Xác định kích cỡ gói tin

KEYSIGHT Technologies cung cấp khá nhiều sản phẩm. Để tìm hiểu thông tin cũng như nâng cấp, đến địa chỉ www.keysight.com. Trên thị trường cũng có nhiều máy phân tích giao thức phần cứng khác như **RADCOM** and **Fluke**.

Port SPAN

Một người dùng phàn nàn về tình trạng mạng, tuy nhiên bạn thấy không có ai trong tòa nhà gặp vấn đề như vậy. Bạn muốn chạy một máy phân tích hệ thống như **Wireshark** trên port để quan sát giao thông ra vào mạng.

Copyright © Howkteam.com

SPAN (Switch Port Analyser – Máy phân tích switch port) có thể giúp bạn trong việc này. **SPAN** cho phép bạn thu thập giao thông từ một port đến một port khác trên cùng switch.

SPAN sao chép tất cả các đơn vị dữ liệu giao thức quy định cho một port và truyền đến port đích SPAN. Một số loại giao thông không được SPAN chuyển tiếp như **BDPUs**, **CDP**, **DTP**, **VTP**, **STP**. Số session của SPAN có thể thiết lập trên switch phụ thuộc vào mô hình. Ví dụ, các switch Cisco 3560 and 3750 chỉ hỗ trợ nhiều nhất 2 sessions SPAN cùng một lúc, trong khi dòng **switch Cisco 6500** hỗ trợ lên đến 16 sessions.

SPAN có thể thiết lập để thu thập giao thông vào, ra hoặc cả hai. Bạn có thể thiết lập nguồn SPAN như một port xác định, một port đơn trong kênh Ether, một kênh Ether hoặc một VLAN. SPAN không thể được thiết lập với một port nguồn của MEC (Multi chassis Ether channel). Bạn cũng không thể thiết lập nguồn của một port đơn hoặc một VLAN. Khi thiết lập nhiều nguồn cho một session SPAN, bạn chỉ cần xác định rõ giao diện của nguồn.

Một điều cần ghi nhớ khi thiết lập SPAN là nếu bạn sử dụng port nguồn có băng thông lớn hơn port đích, trong trường hợp link bị nghẽn, giao thông sẽ dừng lại.

Thiết lập Local SPAN đơn giản

Xem xét hình vẽ dưới đây trong đó một **Router (R1)** được kết nối với switch qua **Switch's Fast Ethernet port 0/1**, port này được thiết lập là port **SPAN** nguồn. Giao thông sao chép từ **FE0/1** sẽ phản ánh **FE0/24** nơi mà **workstation** của chúng ta đang đợi để thu thập giao thông.

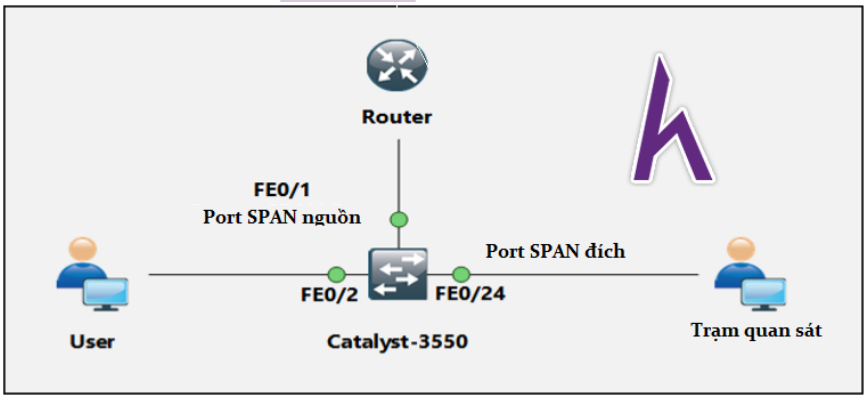


Figure 8-03 SPAN Port

Sau khi chúng ta chạy máy phân tích mạng, bước đầu tiên là thiết lập **Fast Ethernet 0/1** thành port SPAN nguồn và **Fast Ethernet 0/24** thành port SPAN đích. Sau khi thiết lập hai giao diện, LED của port SPAN đích (FE0/24) bắt đầu phát nhanh trong đồng bộ hóa với LED của FE0/1 – một hành vi không lường trước nếu xem xét tình huống tất cả gói tin FE0/1 được sao chép thành FE0/24.

Wiretapping

Wiretapping là quá trình thu thập thông tin bằng cách mắc ống nghe vào dây dẫn như dây điện thoại hay internet. **Wiretapping** hầu hết được thực hiện bởi bên thứ ba để nghe lén đoạn hội thoại. Wiretapping cơ bản là mắc ống nghe vào đường dây điện thoại. **Legal Wiretapping** được gọi là chặn bắt hợp pháp, thường được chính phủ hay các cơ quan an ninh thực hiện.

Wiretapping được chia thành hai loại:

- Wiretapping chủ động

Wiretapping chủ động là quá trình quan sát, thu thập thông tin bằng cách nghe trộm qua dây dẫn. Bên cạnh đó, wiretapping chủ động bao gồm chỉnh sửa đoạn hội thoại.

- Wiretapping thụ động

Quá trình quan sát và thu thập thông tin mà không chỉnh sửa hội thoại.

Copyright © Howkteam.com

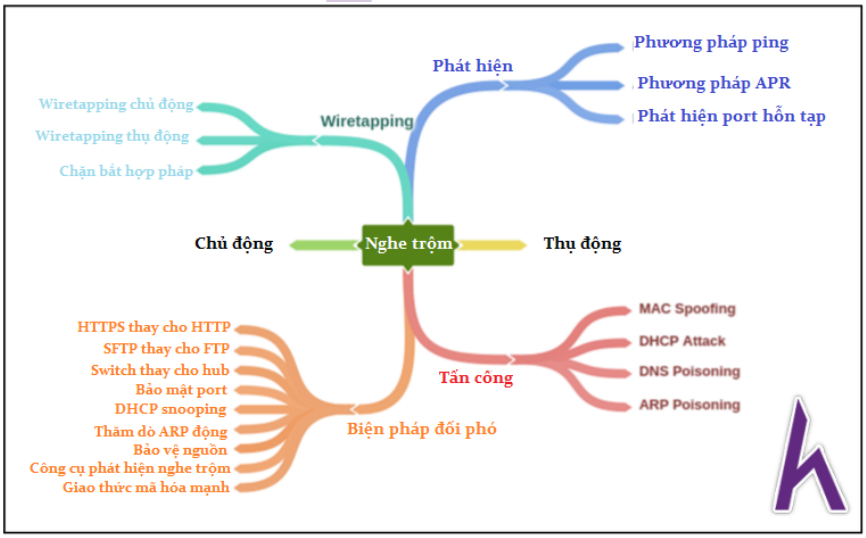
- Chặn bắt hợp pháp

Đây là quá trình wiretapping với đầy đủ giấy phép, cho phép các cơ quan thi hành luật được nghe trộm qua dây dẫn các đoạn hội thoại của user. Tổ chức chuẩn hóa viễn thông đã tiêu chuẩn hóa cổng chặn bắt hợp pháp để phục vụ cho quá trình chặn bắt của các cơ quan.

- Công cụ lên kế hoạch tích hợp tài nguyên (PRISM)

PRISM viết tắt cho **Planning Tool for Resource Integration**, **Synchronization and Management** (công cụ lên kế hoạch tích hợp, đồng bộ hóa và quản lí tài nguyên). **PRISM** là công cụ thiết kế chuyên dụng để thu thập thông tin và quá trình truyền qua American servers. **PRISM** được tạo ra bởi Ban vận hành nguồn đặc biệt (SSO) của Cơ quan an ninh quốc gia (NSA). Mục đích chính của PRISM là nhận diện và quan sát những hội thoại đáng ngờ của mục tiêu. NSA nghe trộm qua dây dẫn giao thông mạng trong nước Mỹ, cũng như dữ liệu lưu trữ ở các server trong nước.

Mindmap



Tấn công MAC

Bảng địa chỉ MAC/ bảng CAM

Media Access Control Address (địa chỉ kiểm soát truy cập phương tiện) hay địa chỉ MAC là địa chỉ vật lí của một thiết bị. Địa chỉ MAC là một số định danh 48-bits duy nhất đặt cho thiết bị hệ thống để giao tiếp ở tầng liên kết dữ liệu. Địa chỉ MAC bao gồm **Object Unique Identifier** (QUI) 24-bits và **Network Interface Controller** (NIC) 24-bits. Nếu có nhiều NIC thì thiết bị sẽ có nhiều địa chỉ MAC khác nhau.

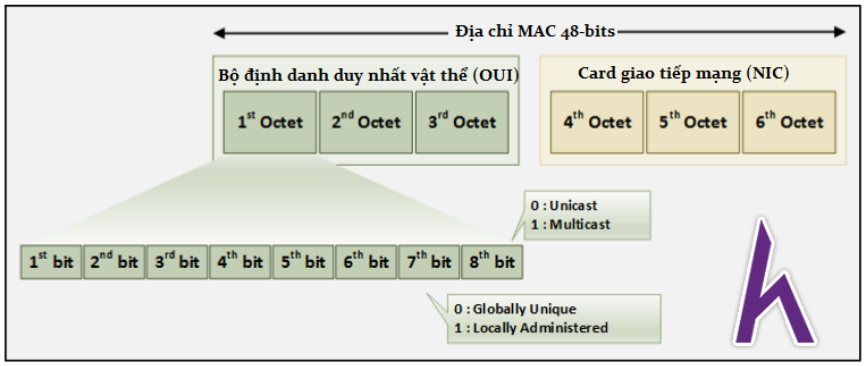


Figure 8-04 MAC-Address

Copyright © Howkteam.com

Bảng địa chỉ **MAC** hay bảng **CAM** (**Content-Addressable Memory**) được sử dụng trong **switch Ethernet** để ghi lại địa chỉ MAC cũng như những thông tin liên quan để chuyển tiếp gói tin. Bảng CAM là bảng ghi lại thông tin của địa chỉ MAC như VLAN liên quan, kiểu học và các thông số port. Các thông số này giúp chuyển tiếp gói tin ở tầng liên kết dữ liệu.

Cách thức hoạt động của bộ nhớ có thể truy cập (CAM)

Học địa chỉ MAC là nhiệm vụ cơ bản của switch. Switch quan sát các frame đến và ghi lại địa chỉ MAC nguồn của những frame này trong bảng địa chỉ MAC. Nó cũng ghi lại port xác định của địa chỉ MAC nguồn. Switch sẽ dựa vào những thông tin này để chuyển tiếp frame thông minh.

> **Chú ý:** máy tính có thể bị tắt hoặc dịch chuyển bất cứ lúc nào. Do đó, switch phải tính thời gian của địa chỉ MAC và xóa nó khỏi bảng nếu không thấy nó một thời gian.

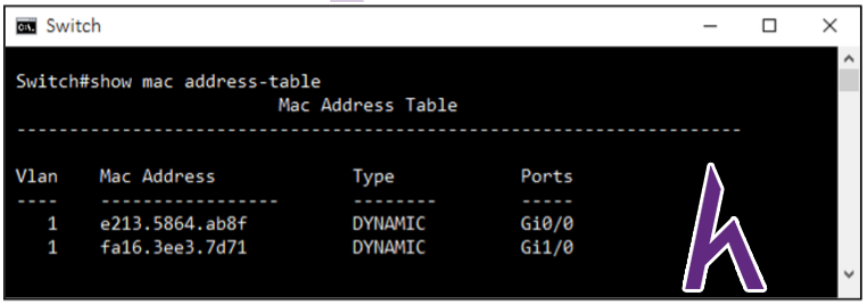


Figure 8-05 MAC-Address Table

Switch hỗ trợ nhiều địa chỉ **MAC** trên tất cả port nên chúng ta có thể kết nối **workstation** cá nhân hoặc nhiều thiết bị qua switch hay router. Dựa vào tính năng địa chỉ động, switch cập nhật địa chỉ nguồn mà các gói tin gửi, gắn nó vào giao diện from which it is received. Do những thiết bị được thêm vào hay xóa đi, chúng được cập nhật rất sôi nổi. Thời gian lão hóa mặc định của địa chỉ MAC là 300 giây. Switch được thiết lập học địa chỉ MAC mặc định.

MAC Flooding

MAC Flooding là một kĩ thuật, trong đó kẻ tấn công gửi ngẫu nhiên những địa chỉ MAC với địa chỉ IP để làm đầy dung lượng lưu trữ của bảng CAM. Như chúng ta đã biết, bảng CAM có độ dài cố định, nên switch sau đó sẽ hoạt động như một hub. Nó sẽ truyền gói tin trên mọi port, giúp kẻ tấn công nghe trộm gói tin dễ dàng. Tài nguyên **Unix / Linux "macof"** cung cấp MAC flooding. MAC nguồn ngẫu nhiên và IP có thể được gửi trên giao diện sử dụng macof.

Đánh cắp switch port

Đây cũng là một kĩ thuật nghe trộm gói tin khác sử dụng **MAC flooding**. Kẻ tấn công sẽ gửi gói tin ARP giả với địa chỉ MAC nguồn của mục tiêu và địa chỉ đích của nó để đóng giả host của mục tiêu, ví dụ host A. Khi những thông tin này chuyển tiếp đến switch, switch sẽ cập nhật bảng CAM. Khi host A gửi gói tin thì switch phải cập nhật lần nữa. Cứ như vậy, khi host A gửi ARP và địa chỉ MAC, switch sẽ gửi gói tin cho kẻ tấn công vì lầm tưởng host A kết nối với port này.

Chống lại tấn công MAC

Bảo mật port được sử dụng để gắn địa chỉ MAC của những thiết bị đã biết với port vật lí và xác định những hành động xâm nhập. Do đó, nếu kẻ tấn công thử kết nối PC của họ với switch port, nó sẽ ngay lập tức ngăn chặn tấn công. trong bảo mật port động, bạn sẽ thiết lập số địa chỉ MAC và switch chỉ hỗ trợ tổng số địa chỉ MAC đó mà không quan tâm đến loại địa chỉ.

Thiết lập bảo mật port

Copyright © Howkteam.com

Cisco Switch cung cấp bảo mật port để phòng tránh tấn công MAC. Bạn có thể thiết lập switch với địa chỉ MAC tĩnh, hoặc MAC động trong một khoảng nhất định, hoặc cả hai. Thiết lập trên **Cisco Switch** dưới đây sẽ hỗ trợ địa chỉ MAC nhất định và 4 địa chỉ phụ. Nếu switch đã học được địa chỉ MAC tĩnh:

Thiết lập bảo mật port

:

```
Switch(config)# interface ethernet 0/0
Switch(config-if)#switchport mode access
Switch(config-if)# switchport port-security
//Enabling Port Security Switch(config-if)# switchport port-security mac-address <mac-address>
//Adding static MAC address to be allowed on Ethernet 0/0
Switch(config-if)# switchport port-security maximum 4
//Configuring dynamic MAC addresses (maximum up to 4 MAC addresses) to be allowed on Ethernet 0/0
Switch(config-if)# switchport port-security violation shutdown
//Configuring Violation action as shutdown
Switch(config-if)#exit
```

Tấn công DHCP

Giao thức thiết lập host động (DHCP)

DHCP là quá trình phân chia động địa chỉ MAC sao cho các địa chỉ này được chỉ định tự động và tái sử dụng khi host không cần chúng. Thời gian **Round Trip (RTT)** đo khoảng thời gian từ khi phát hiện DHCP server đến khi nhận được địa chỉ IP đã thuê.

RTT dùng để đánh giá chất lượng hoạt động của DHCP. Bằng cách sử dụng phiên truyền UDP, DHCP client gửi gói tin **DHCP-Discover** ban đầu bởi vì nó không tin về hệ thống đã kết nối. **DHCP server** phản hồi gói tin **DHCP-Discover** với gói tin **DCHP-Offer** cung cấp thông số thiết lập. DHCP client sẽ gửi tiếp gói tin **DCHCP-request** để yêu cầu thông số thiết lập. Cuối cùng, **DHCP Server** sẽ gửi gói tin **DHCP-Acknowledgement** chứa thông số thiết lập.

DHCPv4 sử dụng hai port khác nhau:

- UDP port 67 cho Server.
- UDP port 68 cho Client.

DHCP Replay agent chuyển tiếp gói tin DHCP từ server đến client và client đến server. **DHCP agent** giúp chuyển tiếp yêu cầu và phản hồi giữa server và client. Khi nhận được tin nhắn DHCP, **Replay agent** sẽ tạo ra một yêu cầu DHCP mới để gửi từ một giao diện khác chứa thông tin cổng mặc định cũng như lựa chọn về thông tin **Replay-Agent** (Option-82). Khi Replay agent nhận được phản hồi từ server, nó sẽ xóa Option 82 và chuyển tiếp lại cho client.

Cách thức hoạt động của **Replay agent** và **DHCPv6** server tương tự như IPv4 Relay agent và **DHCPv4 Server**. DHCP server nhận yêu cầu và chỉ định địa chỉ IP, DNS, thời gian thuê và các thông tin khác cho client trong khi replay server chuyển tiếp tin nhắn DHCP.

Copyright © Howkteam.com

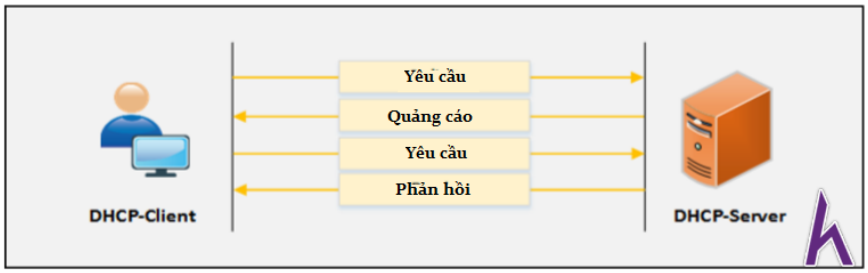


Figure 8-07 IPv6 DHCP process

DHCPv6 sử dụng hai port khác nhau:

- UDP port 546 cho clients.
- UDP port 547 cho servers.

Tấn công DHCP Starvation

Đây là tấn công từ chối dịch vụ trên **DHCP Server**. Trong tấn công này, kẻ tấn công gửi yêu cầu ảo với địa chỉ MAC giả để truyền đến **DHCP Server**, từ đó thuê tất cả địa chỉ IP trong bộ trữ IP. Sau khi tất cả địa chỉ IP được phân phát, những user tiếp theo sẽ không nhận được địa chỉ IP hay gia hạn hợp đồng thuê. Tấn công **DHCP Starvation** có thể được thực hiện bởi các công cụ như "**Dhcpstarv**" hay "**Yersinia**."

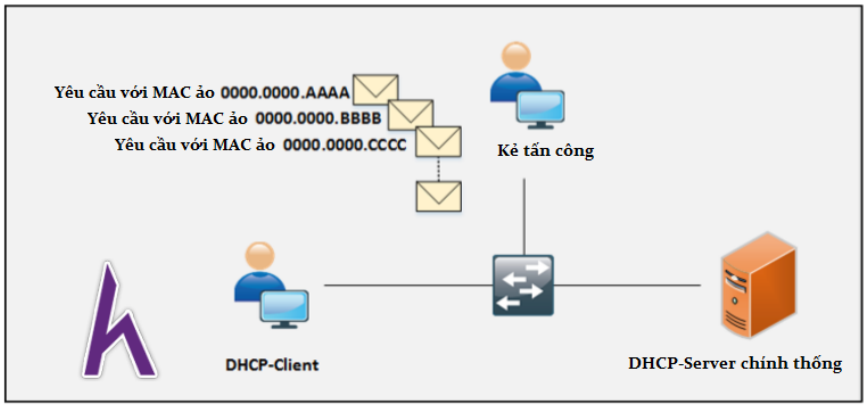


Figure 8-08 DHCP Starvation Attack

Tấn công Rogue DHCP Server

Tấn công này được thực hiện bằng cách triển khai **rogue DHCP Server** trong hệ thống cùng với tấn công starvation. Khi server DHCP chính thống đang bị tấn công từ chối dịch vụ, **DHCP client** không thể nhận được địa chỉ IP. Những gói tin **DHCP Discovery (IPv4)** hoặc **Solicit (IPv6)** tiếp theo được phản hồi bởi **DHCP server** giả với những thông số thiết lập hướng giao thông mạng về phía nó.

Copyright © Howkteam.com

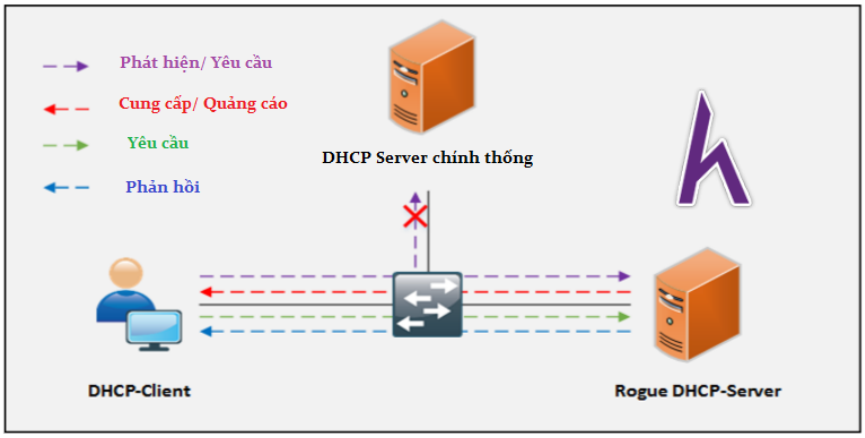


Figure 8-09 Rogue DHCP Server Attack

Chống lại tấn công DHCP Starvation và Rogue Server

DHCP Snooping

Một người có thể dễ dàng đem một **server DHCP** vào môi trường hệ thống, dù vô tình hay hữu ý. **DHCP Snooping** là kĩ thuật phòng tránh việc đó. Để giảm thiểu tấn công, tính năng **DHCP snooping** được kích hoạt trên thiết bị hệ thống để nhận diện những port đáng tin cậy từ những giao thông DHCP chính thống.

Những port khác phản hồi yêu cầu DHCP sẽ bị bỏ qua. Đây là tính năng bảo mật bằng cách lọc tin nhắn DHCP không đáng tin bằng cách xây dựng bảng gắn kết **DHCP snooping**. **DHCP snooping** có khả năng phân biệt giữa giao diện không đáng tin (kết nối với user/host cuối) và giao diện đáng tin (kết nối với **DHCP server** chính thống hoặc thiết bị đáng tin cậy).

Bảo mật port

Kích hoạt bảo mật port cũng giúp giảm thiểu những tấn công này bằng cách giới hạn số lượng địa chỉ MAC trên port có thể học, thiết lập hoạt động vi phạm, thời gian lão hóa, v.v.

Copyright © Howkteam.com