BẢO VỆ MÁY CHỦ CUNG CẤP DỊCH VỤ DHCP BẰNG GIẢI PHÁP PORTSECURITY

ThS. Phan Trần Điền [*]

Trong một hệ thống mạng, các máy tính thường liên lạc với nhau bằng giao thức TCP/IP, do đó chúng phải được cấu hình IP theo một quy tắc nhất định. Với một hệ thống khoảng từ dưới 100 máy tính trở xuống thì việc cấp phát, cài đặt, quản lý các địa chỉ IP thủ công có thể thực hiện được. Tuy nhiên, đối với hệ thống máy lớn từ vài trăm máy tính thì việc sử dụng một dịch vụ như DHCP (Dynamic Host Configuration Protocol) để cấp phát, quản lý địa chỉ IP một cách tự động là hoàn toàn cần thiết, nhằm giúp giảm khối lượng công việc cho quản trị hệ thống. DHCP vô cùng quan trọng đối với hoạt động của hầu hết các hệ thống mạng của các cơ quan, doanh nghiệp. Nhưng trên thực tế vấn đề bảo vệ an toàn cho máy chủ chạy dịch vụ DHCP lại là phần dễ dàng bị bỏ qua nhất trong khâu cấu hình hệ thống.

Trong khuôn khổ bài viết này, người viết trình bày cách bảo vệ máy chủ cung cấp dịch vụ DHCP bằng giải pháp portsecurity trên thiết bị chuyển mạch (switch) của hãng Cisco như sau:

1. Một số ưu điểm của DHCP

DHCP là giao thức cung cấp phương pháp thiết lập các thông số TCP/IP cần thiết cho hoạt động của mạng. Dịch vụ DHCP gồm: Máy chủ chạy dịch vụ DHCP (DHCP Server) và máy trạm chạy dịch vụ DHCP (DHCP Client). Quá trình trao đổi thông tin giữa DHCP Server và DHCP Client thường được thực hiện:

DHCP client muốn nhận một địa chỉ IP mới sẽ gửi lên toàn mạng (gói tin broadcast) thông điệp DHCP Discover chứa địa chỉ MAC (Media Access Control) của mình để tìm kiếm sự hiện diện của máy chủ DHCP Server.

Nếu có một DHCP Server có cùng lớp mạng với DHCP Client thì DHCP Server phản hồi lại với thông điệp DHCP Offer có chứa địa chỉ IP và các thiết lập TCP/IP khác như một lời đề nghị cho thuê địa chỉ đó.

- DHCP Client sẽ gửi lại cho DHCP Server đó một thông điệp DHCP như là một lời chấp thuận thuê địa chỉ IP đó.

[*] ***Trưởng Bộ môn Tin học, Khoa Đại cương, Học viện Cán bộ Thành phố Hồ Chí Minh***

- Cuối cùng, DHCP Server sẽ gửi lại cho DHCP Client thông điệp DHCP Acknowledgment để xác nhận lần cuối hợp đồng cho thuê địa chỉ IP.

Sau các bước trên, máy tính trạm có thể sử dụng IP vừa được thuê để truyền thông với các máy tính khác trên hệ thống mạng. Sử dụng dịch vụ DHCP sẽ có các ưu điểm sau: Quản lý TCP/IP tập trung, giúp người quản trị dễ quản lý, cấu hình, khắc phục khi có lỗi xảy ra trên các máy DHCP client. Người quản trị không phải đến từng máy người dùng để cấp phát địa chỉ IP.

2. Tấn công vào dịch vụ DHCP

Trong quá trình thông điệp giữa DHCP Server và DHCP Client không có sự xác thực hay kiểm soát truy cập. DHCP Server không thể biết được rằng việc trao đổi với một DHCP client bất hợp pháp hay không và DHCP Client cũng không thể biết DHCP Server mà mình đang liên lạc có hợp pháp không. Chính vì vậy sẽ có thể xảy ra hai tình huống mất an toàn thông tin, khi DHCP Client là một máy trạm bất hợp pháp:

- *Thứ nhất là*, khi kẻ tấn công thỏa hiệp thành công với một DHCP Client hợp pháp trong hệ thống mạng, sau đó thực hiện việc cài đặt, thực thi một chương trình. Chương trình này liên tục gửi tới DHCP Server các gói tin yêu cầu xin cấp địa chỉ IP với các địa chỉ MAC nguồn không có thực, cho tới khi dải IP có sẵn trên DHCP Server cạn kiệt vì bị nó thuê hết. Điều này dẫn tới việc DHCP Server không còn địa chỉ IP nào để cho các DHCP Client hợp pháp thuê, khiến dịch vụ bị ngưng trệ, các máy trạm khác không thể truy nhập vào hệ thống mạng để truyền thông với các máy tính trong mạng.
- *Thứ hai là*, khi DHCP Server là một máy chủ bất hợp pháp, kẻ tấn công phá vỡ được các hàng rào bảo vệ mạng và đoạt được quyền kiểm soát DHCP Server, nó có thể tạo ra những thay đổi trong cấu hình của DHCP Server theo ý muốn. Kẻ tấn công có thể tấn công hệ thống mạng theo các cách sau:
  + Tấn công DoS (Denial of Service) hệ thống mạng: Kẻ tấn công thiết lập lại dải IP, subnet mask của hệ thống để các máy trạm hợp pháp không thể đăng nhập vào hệ thống mạng được, tạo ra tình trạng DoS trong mạng.
  + Tấn công giả mạo hệ thống phân tên miền (Domain Name System): Kẻ tấn công đổi các thiết lập Domain Name System (DNS) để chuyển hướng yêu cầu phân dải tên miền của Client tới các DNS giả mạo, kết quả là Client có thể bị dẫn dụ tới các website giả mạo được xây dựng nhằm mục đích đánh cắp thông tin tài khoản của người dùng hoặc website có chứa các mã độc, virus, trojan... sẽ được tải về máy Client.

3. Bảo vệ máy chủ cung cấp dịch vụ DHCP bằng giải pháp PortSecurity

Với tấn công từ chối dịch vụ bằng cách sử dụng một DHCP Client bất hợp pháp và giả mạo DNS, ta có thể khắc phục bằng cách sử dụng các switch có tính năng bảo mật cao, giúp hạn chế số lượng địa chỉ MAC có thể sử dụng trên một cổng. Mục đích là để ngăn chặn việc có quá nhiều địa chỉ MAC sử dụng trên một cổng đó trong một khoảng thời gian giới hạn, nếu vượt qua giới hạn này cổng sẽ bị đóng lại ngay lập tức. Thời gian cổng hoạt động trở lại tùy thuộc vào giá trị mặc định do người quản trị mạng thiết lập.

Hiện nay hãng Cisco đã có giải pháp PortSecurity để ngăn chặn tấn công từ chối dịch vụ DHCP bằng cách sử dụng một DHCP Client bất hợp pháp. Chức năng PortSecurity sẽ giới hạn đầu vào interface bằng cách hạn chế và xác định địa chỉ Media Access Control (MAC) là mã duy nhất được gán bởi nhà sản xuất cho từng phần cứng mạng và là duy nhất cho các thiết bị (như cạc không dây hoặc cạc Ethernet) của các máy trạm được phép truy cập vào. Khi chỉ định địa chỉ secure MAC đến một cổng bảo mật, cổng không chuyển tiếp các gói tin với địa chỉ nguồn bên ngoài nhóm các địa chỉ đã xác định. Nếu hạn chế số lượng địa chỉ secure MAC tới một cổng và chỉ định một địa chỉ secure MAC, các máy trạm thuộc port đó được đảm bảo đầy đủ băng thông. Nếu một port secure với số lượng tối đa các địa chỉ secure MAC được đạt tới, khi địa chỉ MAC của các máy trạm còn lại cố gắng truy cập vào cổng mà khác với các địa chỉ secure MAC đã xác định, thì vi phạm (violation) bảo mật xảy ra. Khi vi phạm xảy ra ta có thể cấu hình các hành động ứng với các vi phạm đó cụ thể là: Shutdown: Các cổng trên thiết bị chuyển mạch sẽ được đưa vào trạng thái lỗi và bị tắt đi; Restric: Các cổng trên thiết bị chuyển mạch ở trạng thái hoạt động mặc dù địa chỉ MAC kết nối bị sai. Tuy nhiên các gói tin đến cổng này đều bị hủy và sẽ có một bản thông báo về số lượng gói tin bị hủy; Protect: Các cổng trên thiết bị chuyển mạch vẫn ở trạng thái hoạt động như restrict, các gói tin đến cổng này đều bị hủy và không có thông báo về việc hủy bỏ gói tin này.

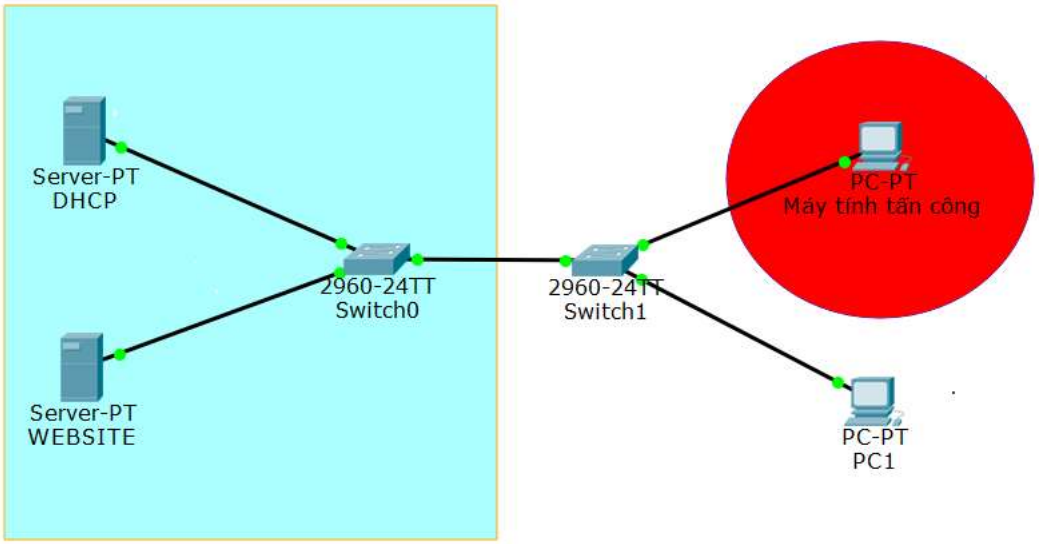
Các bước để cấu hình PortSecurity trên thiết bị Switch1 (2960-24TT-Switch1):

– Vào cấu hình mode access trên interfaces Fa0/2 và bật tính năng Port Security

```
HVCB(config)#interface fa0/2
```

HVCB(config-if)#switchport mode access

HVCB(config-if)#switchport port-security



– Qui định tối đa một địa chỉ MAC trên cổng Fa0/2 của Switch

HVCB(config-if)#switchport port-security maximum 1

– Gán địa chỉ MAC của PC đến Port được kết nối đến Switch1

HVCB(config-if)#switchport port-security mac-address *0001.9767.8376*

– Cư xử của Switch1 sau khi phát hiện sai phạm là Shutdown Port.

HVCB (config-if)#switchport port-security violation shutdown

– Kiểm tra

```
HVCB#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------
        Fa0/2        1           1                0          Shutdown
---------------------------------------------------------------------
```

Tóm lại, với việc ứng dụng dịch vụ DHCP luôn mang đến rất nhiều ưu điểm, bên cạnh đó cũng là những nguy cơ luôn đe dọa về an toàn thông tin không nhỏ. Sử dụng dịch vụ DHCP phải đi liền với các phương pháp bảo mật cho hệ thống. Vì vậy, việc triển khai giải pháp PortSecurity cho hệ thống mạng nhằm để phòng ngừa và bảo vệ máy chủ cung cấp dịch vụ DHCP là hết sức cần thiết./.

Tài liệu tham khảo

[1]. Lê Đức Thịnh (2015), Cấu hình port security như thế nào. VnPro. Địa chỉ: http://www.vnpro.vn/thu-vien/cau-hinh-port-security-nhu-the-nao-2264.html

[2]. Cisco, Chapter: Configuring Port Security. Địa chỉ: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

[3]. KS. Phạm Thành Công (2013), Tấn công vào dịch vụ DHCP. Ban cơ yếu chính phủ an toàn thông tin. Địa chỉ: http://antoanthongtin.vn/Detail.aspx?CatID=1177d915-8953-48c8-91fd-51b954bd821d&NewsID=8e2d8023-67e3-4ae4-8720-f1ac9dcfffe3