KẾT HỢP KỸ THUẬT VLAN-ACCESS LIST NÂNG CAO HIỆU QUẢ BẢO MẬT MẠNG LAN ẢO

Lê Hoàng Hiệp*, **Phạm Thị Liên**
Trường Đại học Công nghệ thông tin & Truyền thông – ĐH Thái Nguyên

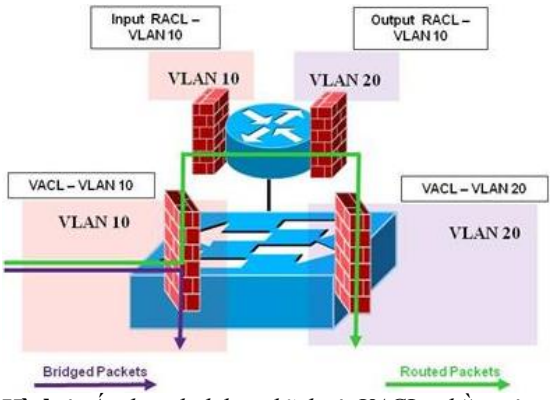
TÓM TẮT

Khi số lượng VLAN nhiều, việc quản lý các IP traffic yêu cầu hỗ trợ mức độ cơ bản về bảo mật cho các truy cập mạng trở nên khó khăn hơn, người quản trị mạng khi đó cần một kỹ thuật nào đó vừa tận dụng được hạ tầng sẵn có vừa đáp ứng được các yêu cầu về hiệu năng quản trị mạng, chi phí, băng thông,…vừa quản trị được các mạng VLAN tốt hơn, khi đó có thể dùng tới kỹ thuật VLAN-Access List thể hiện ở tính năng lọc các gói tin qua Router tương tự như kỹ thuật Access List cho các mạng LAN cùng với việc kết hợp các tính năng bảo mật được tích hợp trên các thiết bị mạng có thể đem lại hiệu quả bảo mật cao hơn nhiều so với việc không ứng dụng VLAN-Access List.

Từ khóa: *LAN, VLAN, Access List, VLAN-Access List, Vlan Access-map*

GIỚI THIỆU

VLAN ACLs (VACLs) là một dịch vụ cho phép tạo và quản lý danh sách truy cấp dựa vào địa chỉ MAC, IP. Người quản trị mạng có thể cấu hình VACLs để kiểm tra các gói tin lưu thông trong nội bộ một VLAN, hoặc giữa các VLAN với nhau. VACLs không quản lí truy cập theo hướng (In, Out) như khi áp dụng kỹ thuật Access List cho các LAN. VACLs dùng Access Map để chứa danh sách tuần tự một hoặc nhiều gói tin (entry) về việc quản lí truy cập. Mỗi gói tin trong bản đồ truy cập mô tả việc kiểm tra gói tin dựa vào IP hoặc MAC để áp dụng cho một hành động nào đó đối với những gói tin [1] [5].



Hình 1. *Áp dụng linh hoạt kỹ thuật VACLs nhằm nâng cao hiệu quả bảo mật trong quản trị mạng LAN ảo*

Các gói tin đều được đánh số thứ tự nên có thể cấu hình ưu tiên cho các gói tin phù hợp với một yêu cầu nào đó. Khi các gói tin đi qua thiết bị sẽ được kiểm tra thông qua VACLs dựa vào bản đồ truy cập đã được cấu hình mà thiết bị sẽ quyết định có chuyển tiếp gói tin đi hay không. Những gói tin trong VLAN Access Map cung cấp các hành động đối với:

- Forward: Hành động này sẽ cho phép gói tin được chuyển tiếp qua Switch.
- Redirect: Gói tin sẽ được chuyển hướng sang một hoặc nhiều giao diện (interface) được chỉ định.
- Drop: Với một gói tin vi phạm thì hành động này cho phép hủy gói tin ngay lập tức và chúng ta có thể lưu trạng thái (logs) về việc hủy các gói tin này.

Vấn đề đặt ra, với ACLs bình thường khi cấu hình trên Router thì không thể ngăn chặn hoặc cho phép lưu lượng qua lại giữa các VLAN, nhưng khi áp dụng kỹ thuật VACLs điều này hoàn toàn có thể thực hiện được, do đó tính năng này sẽ giúp nâng cao chính sách bảo mật cho hệ thống mạng LAN ảo (VLAN) [5].

NHẬN DIỆN MỘT SỐ NGUY CƠ TẤN CÔNG MẠNG LAN VÀ MẠNG LAN ẢO

Tấn công mạng LAN

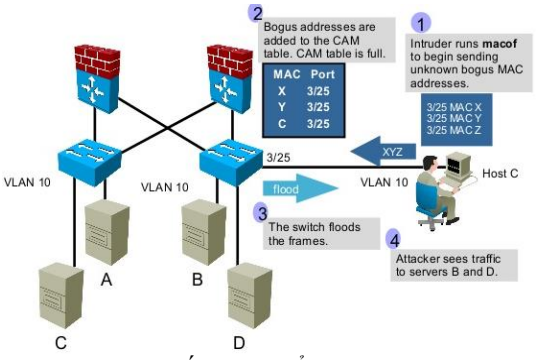
Dưới đây là một số nguy cơ tiềm tàng mà kẻ xấu (Hacker) có thể dựa vào đặc điểm yếu này để thực hiện tấn công vào lỗ hổng bảo mật của mạng LAN [2]:

Kiểu tấn công làm tràn MAC

- Bảng CAM (Content Addressable Memory) lưu trữ các địa chỉ MAC của các cổng (port),

* *Tel: 0984 666500; Email: lhhiep@ictu.edu.vn*

và các tham số VLAN trong Switch. Không gian nhớ trong bảng CAM là hạn chế nên có nguy cơ tràn bảng CAM. Kiểu tấn công làm tràn MAC sẽ cố gắng làm tràn bảng CAM của các Switch, khi đó Switch sẽ cư xử như các hub.



Hình 2. *Tấn công kiểu MAC flooding*

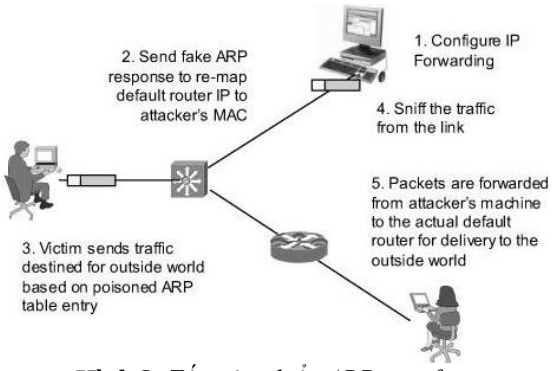
Một cuộc tấn công kiểu này (Hình 2) trông giống như lưu lượng từ hàng ngàn máy tính được chuyển đến một cổng, nhưng thực tế là nó chỉ đến từ một máy giả mạo địa chỉ MAC của hàng ngàn máy tính (host) giả mạo.

Tấn công làm ngập lụt bảng MAC là một trong những kĩ thuật tấn công phổ biến nhất ở Layer 2. Trong kiểu tấn công này thì Switch đã bị "ngập lụt" với các gói tin của các địa chỉ MAC khác nhau, do đó làm tiêu hao bộ nhớ trong Switch, lúc này Switch sẽ trở thành Hub. Do đó người dùng bất hợp pháp có thể sử dụng một công cụ Packet Sniffer để thâu tóm các dữ liệu nhạy cảm trong đó.

ARP Spoofing

ARP spoofing, ARP cache poisoning, hay ARP poison routing, là một kỹ thuật qua đó kẻ tấn công giả lập 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.

ARP spoofing (Hình 3) có thể cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng, hoặc dừng tất cả lưu lượng. Thông thường cuộc tấn công này được sử dụng như là một sự mở đầu cho các cuộc tấn công khác, chẳng hạn như tấn công từ chối dịch vụ (DDos), tấn công Man-in-the-middle attack, hoặc các cuộc tấn công cướp liên lạc dữ liệu [1].

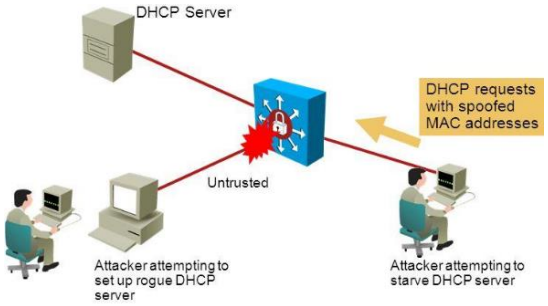


Hình 3. *Tấn công kiểu ARP spoofing*

Cuộc tấn công này chỉ có thể dùng trong các mạng dùng Address Resolution Protocol, và giới hạn trong các mạng cục bộ [2].

Tấn công vào dịch vụ DHCP

Tuy có nhiều ưu điểm, nhưng giao thức DHCP hoạt động lại khá đơn giản, suốt quá trình trao đổi 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 nó đang liên lạc với một DHCP Client bất hợp pháp hay không, ngược lại DHCP Client cũng không thể biết DHCP Server đang liên lạc có hợp pháp không.



Hình 4. *Tấn công kiểu DHCP spoofing*

Như vậy sẽ có hai tình huống xảy ra:

- Khi DHCP Client là một máy trạm bất hợp pháp:

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.

Trường hợp tấn công này chỉ làm cho các máy tính đăng nhập vào hệ thống mạng (sau khi bị tấn công) không thể sử dụng dịch vụ DHCP, dẫn đến không vào được hệ thống mạng. Còn các máy trạm khác đã đăng nhập trước đó vẫn hoạt động bình thường.

Đây là kiểu tấn công từ chối dịch vụ DHCP dễ dàng nhất mà kẻ tấn công có thể thực hiện. Kẻ tấn công chỉ cần rất ít thời gian và băng thông là có thể thực hiện được cuộc tấn công này.

- *Khi DHCP Server là một máy chủ bất hợp pháp:*

Nếu 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 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.

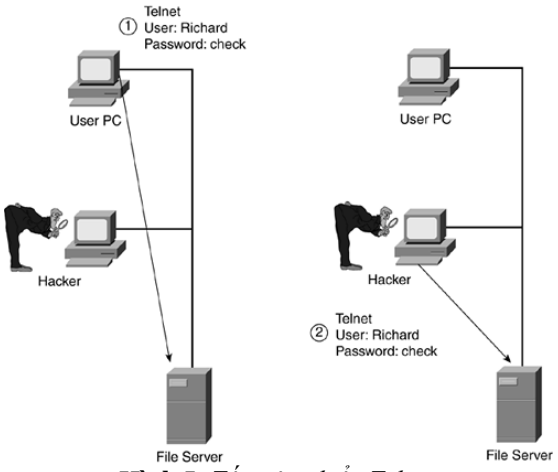
Tấn công theo kiểu DNS redirect: Kẻ tấn công đổi các thiết lập DNS để chuyển hướng yêu cầu phân dải tên miền của Client tới các DNS giả mạo, kết quả là Client có thể bị dẫn dụ tới các website giả mạo được xây dựng nhằm mục đích đánh cắp thông tin tài khoản của người dùng hoặc website có chứa các mã độc, virus, trojan... sẽ được tải về máy Client.

Tấn công theo kiểu Man-In-The-Middle: Kẻ tấn công thay đổi Gateway mặc định trỏ về máy của chúng, để toàn bộ thông tin mà Client gửi ra ngoài hệ thống mạng sẽ được chuyển tới máy này thay vì tới Gateway mặc định thực sự. Sau khi xem được nội dung thông tin, gói tin sẽ được chuyển tiếp đến Gateway thực sự của mạng và Client vẫn truyền bình thường với các máy ngoài mạng mà người dùng không hề biết họ đã để lộ thông tin cho kẻ tấn công.

Nhược điểm của cách tấn công này là kẻ tấn công chỉ có thể xem trộm nội dung thông tin của gói tin gửi ra ngoài mạng mà không thể xem nội dung thông tin của gói tin gửi cho Client từ bên ngoài mạng.

Tấn công Telnet

TELNET (viết tắt của TErminaL NETwork) là một giao thức mạng (network protocol) được dùng để truy cập từ xa đến một thiết bị mạng (Switch, Router, Server...) để quản trị. Telnet là một giao thức giữa Client-Server, dựa trên một kết nối tin cậy. Giao thức này hoạt động ở tầng 7 (layer 7) và sử dụng giao thức TCP cổng 23.



Hình 5. *Tấn công kiểu Telnet*

Tuy nhiên Telnet không bảo mật vì những lý do sau:

- Telnet, theo mặc định, không mã hóa bất kỳ dữ liệu được gửi qua kết nối (bao gồm cả mật khẩu), và vì vậy có khả năng bị nghe trộm các thông tin liên lạc và từ đó Hacker có thể tóm được mật khẩu quản trị và có thể chặn bắt các gói tin đi qua bằng các công cụ phân tích gói tin như Wireshark.

- Hầu hết các thao tác của Telnet không có chứng thực rằng sẽ đảm bảo thông tin liên lạc được thực hiện giữa hai bên như mong muốn và không bị chặn ở giữa.

- Rất nhiều lỗ hổng bảo mật đã được phát hiện trong những năm qua khi sử dụng câu lệnh thông thường như telnet, vì thế telnet là giao thức rất dễ bị tấn công bằng các kỹ thuật: Đánh hơi phiên telnet (Telnet communication sniffing), Tấn công vét cạn (Telnet brute force attack), tấn công từ chối dịch vụ (Telnet DoS – Denial of Service).

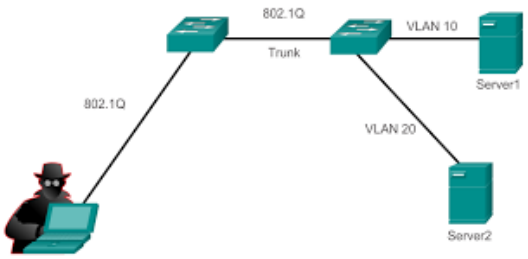
Telnet brute force attack: kẻ tấn công sử dụng danh sách các mật khẩu phổ biến và một tool được thiết kế để thiết lập một phiên telnet, đăng nhập bằng mật khẩu nằm trong danh sách từ điển. Tool này có thể kết hợp các từ (word) tuần tự với nhau để từ đó có thể dò ra mật khẩu (password). Nếu có thời gian thì kiểu tấn công này sẽ có thể phá được tất cả các mật khẩu được sử dụng.

Telnet DoS - tấn công từ chối dịch vụ. Các cuộc tấn công DoS là một cách để phá vỡ truyền thông của hai thiết bị mạng bằng cách sử dụng tất cả băng thông đang có. Để làm như vậy kẻ tấn công gửi nhiều gói dữ liệu không đúng với quy định của giao thức TCP. Cụ thể ở đây là kẻ tấn công có thể sử dụng kỹ thuật SYN-FLOOD. Khi các máy tính bị nhiễm mã độc sẽ chạy ứng dụng Telnet trên các máy tính đó để tạo ra kết nối dạng half-open với một thiết bị mạng, làm cho kênh đăng nhập (line telnet) bị chiếm dụng trong thời gian dài, do vậy người quản trị mạng không thể login vào thiết bị.

Tấn công mạng VLAN

VLAN (Virtual LAN) là mạng LAN ảo, một công nghệ được sử dụng phổ biến trong các mạng LAN của doanh nghiệp với mục tiêu làm gia tăng tính bảo mật cho mạng, tiết kiệm chi phí đầu tư thiết bị, tăng hiệu năng thiết bị và làm đơn giản hóa vấn đề quản lý mạng. Tuy nhiên nếu cấu hình sai (lỗi cấu hình) thì có thể dẫn tới những nguy cơ về an ninh. Có 2 kiểu tấn công VLAN là VLAN Hoping và VLAN Double Tagging [1] [2] [5].

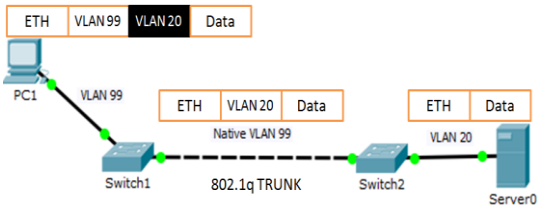
Kiểu tấn công VLAN Hopping Spoofing:



Hình 6. *VLAN hopping spoofing*

Trong Hình 6, kết nối giữa 2 Switch là kết nối kiểu trunk, sử dụng chuẩn đóng dữ liệu gói là giao thức 802.1Q. Kết nối trunk cho phép lưu lượng của nhiều VLAN chạy qua, ví dụ lưu lượng đến VLAN 10 (đến Server1) và VLAN 20 (đến Server2) có thể đi qua kết nối trunk giữa 2 Switch. Tuy nhiên để truy cập vào Server1 thì máy của kẻ tấn công phải nằm ở VLAN 10, còn muốn truy cập đến Server2 thì máy của kẻ tấn công phải thuộc VLAN 20. Tuy nhiên có một cách khác là đánh lừa Switch rằng máy tính của kẻ tấn công là một Switch, từ đó thiết lập kết nối trunk từ máy kẻ tấn công đến Switch. Để đánh lừa, kẻ tấn công sẽ chạy một phần mềm giả lập giao thức DTP (Dynamic Trunking Protocol) trên máy tính của kẻ tấn công. Nếu trạng thái cổng của Switch để ở chế độ mặc định là Dynamic Auto thì kẻ tấn công sẽ cấu hình phần mềm chạy DTP ở chế độ Dynamic Desirable hoặc Trunk, khi đó kết nối từ máy của kẻ tấn công đến Switch là kết nối trunk (Hình 7). Như vậy Hacker có thể truy cập vào các VLAN khác nhau, từ đó truy cập được vào Server1 và Server2.

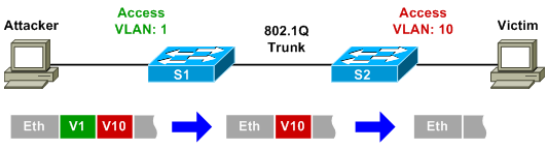
Kiểu tấn công VLAN double tagging



Hình 7. *VLAN double tagging*

Giả sử kẻ tấn công muốn truy cập bất hợp pháp vào Server nằm ở VLAN 20, tuy nhiên máy của Hacker lại nằm ở VLAN 99 (native VLAN). Vậy làm thế nào để truy cập vào Server?

Kẻ tấn công sẽ gắn thêm một tag VLAN 20 vào trong frame Ethernet gửi đến Switch 1. Swich 1 nhận thấy frame này thuộc VLAN 99 nên nó loại bỏ tag VLAN 99 và gửi frame lên đường trunk mà không gắn tag cho frame này bởi vì frame này thuộc native VLAN. Như vậy nghiễm nhiên frame này bây giờ thuộc VLAN 20. Khi Switch 2 nhận được frame VLAN 20, nó sẽ forward đến Server nằm ở VLAN 20. Như vậy kẻ tấn công đã truy cập được vào Server nằm ở VLAN 20 mặc dù máy của kẻ tấn công nằm ở VLAN 99.



Hình 8. *VLAN Hopping with Double Tagging*

Những kẻ tấn công gửi các gói tin được gắn 2 tag 802.1Q đến Switch2 (Hình 8). Tất nhiên những kẻ tấn công không kết nối được với cổng trunk, mà sử dụng một Switch giả mạo để chuyển đổi Switch của mình sang chế độ trunking. Sử dụng trunk encapsulation để lừa

các Switch tạo các frame sang qua các VLAN khác. Frame thực với một số dữ liệu độc hại đầu tiên trong 2 tag 802.1Q với VLAN ID của VLAN mục tiêu (VLAN 20). Sau đó frame gắn tag 802.1Q giả mạo thứ 2 được bổ sung truy cập Vlan ID của kẻ tấn công (VLAN 10). Khi Switch 2 nhận được frame được gắn 2 tag, nó quyết định đẩy qua cổng trunk. Điều này là do tag VLAN 10 có cùng VLAN ID như native vlan trên cổng trunk. Các tag VLAN 10 được gỡ bỏ khi frame đã được gửi trên cổng trunk . Switch sẽ gửi tất cả các gói tin khi gỡ bỏ các tag native VLAN. Do đó tag VLAN 20 được chuyển sang Switch rồi tag giả mạo này tiếp tục được gỡ bỏ và gói tin được chuyển đến VLAN 20. Lúc đó những kẻ tấn công đã gửi thành công gói tin từ VLAN 10 đến VLAN 20 thông qua chuyển mạch lớp 2 mà không cần sử dụng định tuyến.

KỸ THUẬT CẤU HÌNH VLAN-ACCESS LIST

Bên cạnh việc áp dụng các giải pháp bảo mật mạng LAN cơ bản, giải pháp ứng dụng kỹ thuật VACLs sẽ làm tang khả năng bảo mật cho mạng VLAN nói riêng và mạng LAN nói chung.

Trên thiết bị Switch, đăng nhập, chuyển qua chế độ toàn cục, thực hiện các bước sau để áp (gán) lệnh thực thi Vlan-Access List như sau [5]:

Tạo Vlan Access Map:

Switch(config)#vlan access-map {map-name}{sequence-number}

Đưa ACL vào:

Switch(config-access-map)#match {ip\|ipv6\|mac} address {ip-accesslist}

Định nghĩa các hành động cho gói tin

Switch(config-access-map)#action {forward\|drop\|redirect}

Áp dụng lên các Vlan:

Switch(config)#vlan filter {map-name} vlan-lít {list}

Gỡ bỏ cấu hình:

Switch(config)#no vlan access-map {map-name} {sequence-number}

Để thực hiện kiểm tra cấu hình VACLs, trên thiết bị Switch, đăng nhập, chuyển qua chế đặc quyền, thực hiện các bước sau để áp dụng (gán) lệnh kiểm tra Vlan-Access List như sau:

Hiển thị ACL được cấu hình:

Switch#show running-config aclmrg

Hiển thị thông tin VACLs áp dụng cho VLAN:

Switch#show vlan filter

Hiển thị các entry trong Access-Map:

Switch#show vlan access-map

SỬ DỤNG KỸ THUẬT VLAN-ACCESS LIST TĂNG KHẢ NĂNG BẢO MẬT MẠNG VLAN

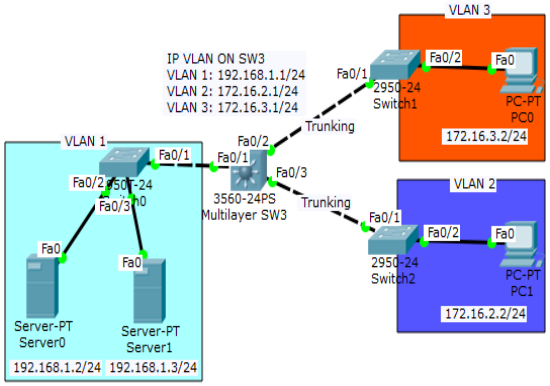
Bên cạnh các giải pháp truyền thống khác để bảo vệ mạng LAN như sử dụng tường lửa (Firewall), thiết lập mạng riêng ảo VPN hay sử dụng hệ thống phát hiện và ngăn ngừa xâm nhập mạng IDS/IPS,… người quản trị còn có thể ứng dụng tối đa tính năng bảo mật trong mạng VLAN [1] [2] [4] [5].

Khi người quản trị mạng thực hiện cấu hình VLAN cho mạng LAN, lúc đó nếu như một VLAN bị tấn công sẽ không gây ảnh hưởng tới VLAN khác vì mỗi VLAN là một miền quảng bá (Broadcast Doamain) riêng biệt.

Trong bài báo này, tác giả sẽ tập trung phân tích, áp dụng tính linh hoạt khi sử dụng kỹ thuật VLAN-Access List cho các mạng LAN ảo (VLAN) nhằm nâng cao tính hiệu quả bảo mật, giảm chi phí vận hành, tận dụng tài nguyên hệ thống.

Đặt vấn đề

Để minh chứng cho hiệu quả khi áp dụng VLAN-Access làm tăng tính bảo mật mạng LAN ảo, dưới đây tác giả sử dụng mô hình thực nghiệm như sau:



Hình 9. *Mô hình thực nghiệm*

Mô hình này (Hình 9) được sử dụng để minh họa việc giải quyết bài toán bảo mật nhỏ như

sau: cấm (deny) việc người dùng truy nhập web từ PC1 tới máy Server 0 nhưng cho phép toàn bộ các lưu lượng (traffic) còn lại được phép (ví dụ, vẫn có thể PING, email, telnet,…).

Thực nghiệm:

Dưới đây sử dụng hai trường hợp: khi không áp dụng VACL và trường hợp có áp dụng VACL để từ đó có đánh giá so sánh về hiệu quả bảo mật của VACL trong trường hợp này.

Trường hợp không sử dụng kỹ thuật VACL:

Với mô hình thực nghiệm như đã nói (Hình 9), mô hình mạng không có thiết bị định tuyến (Router). Trong trường hợp người quản trị muốn sử dụng tính năng bảo mật sẵn có (là trọng tâm phân tích của bài báo này nhằm nâng cao tính bảo mật cho mạng LAN ảo mà không sử dụng thêm các thiết bị bảo mật chuyên dụng hoặc các giải pháp phải trả phí khác) như Access Control List trên router thì điều này là không thể thực hiện được. Hơn nữa với các mô hình mạng thiết kế phổ biến theo kiểu phân cấp trên thực tế hiện nay, từ một router nối tới nhiều Switch layer 2 và Switch layer 3, bên trong đó lại có rất nhiều mạng VLAN, khi đó việc áp dụng kỹ thuật Access Control List truyền thống là điều rất khó để giải quyết các tình huống tương tự như trong bài toán này, gây ra sự phức tạp lớn trong việc quản trị và thực thi.

Trường hợp áp dụng kỹ thuật VACL:

Để giải quyết bài toán này, việc áp dụng kỹ thuật VACL là điều cần thiết để giải quyết các tình huống tương tự với hệ thống mạng có nhiều thiết bị chuyển mạch (Switch). Trên thiết bị Switch Layer 3, thực hiện cấu hình VACL như sau:

Switch(config)#access-list 120 deny tcp 172.16.2.0 0.0.0.255 host 192.168.1.2 eq www

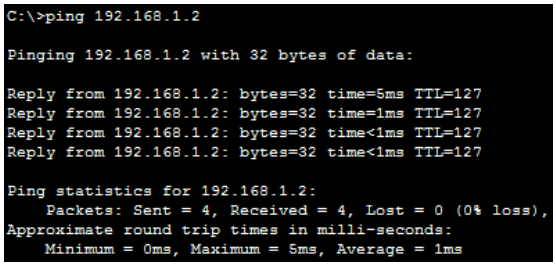
Switch(config)# access-list 120 permit ip any any

Switch(config)#interface vlan 1

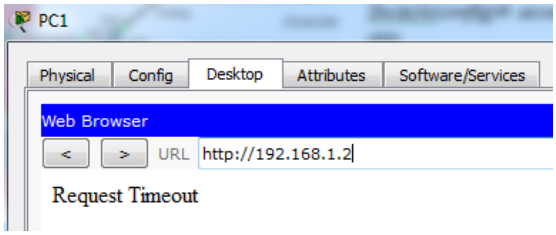
Switch(config-if)#ip access-group 120 out

Kết quả sau khi áp dụng kỹ thuật VACL trên Switch đã giải quyết được yêu cầu của bài toán:

+ Thực hiện lệnh Ping từ PC1 tới Server0 thành công:



+ Việc cấm truy nhập web từ PC1 tới Server0 thành công:



Đánh giá kết quả:

Bằng việc áp dụng kỹ thuật VACLs phù hợp trên thiết bị Switch, khả năng bảo mật trong mạng VLAN tăng lên đáng kể, tận dụng được tính năng bảo mật sẵn có của Switch, giảm chi phí vận hành,... Hoặc trong các trường hợp nếu hệ thống mạng bị kẻ xấu tấn công sử dụng một trong các kiểu tấn công được trình bày trong mục 2, người quản trị rất khó để kiểm soát các lưu lượng vào ra trong hệ thống hoặc tìm ra được các cảnh báo, nguy cơ mất an toàn đang đến. Tuy nhiên, khi áp dụng linh hoạt kỹ thuật VACL, người quản trị có thể kiểm soát lưu lượng ra vào (in/out) rất chi tiết trong mạng LAN ảo trên thiết bị Switch (tính năng mà Router chưa hỗ trợ, hoặc là với mạng có ít hoặc không có thiết bị router khi đó VACL càng quan trọng), để từ đó nắm được tình trạng hiện thời của hệ thống mạng và có phương án xử lý kịp thời [1] [5].

KẾT LUẬN

Như đã trình bày, VACLs là một trong những phương pháp nâng cao tính bảo mật trong mạng (cụ thể là trong mạng LAN). Kỹ thuật này cho phép kiểm soát lưu lượng chạy qua thiết bị Switch. Khi cấu hình VACLs người quản trị có thể phân loại lưu lượng từ các giao thức như: IP, TCP, HTTP,… Tùy vào chính sách mà người quản trị mạng áp đặt vào VACLs có thể loại bỏ hoặc cho phép các loại dữ liệu (theo cấu hình) được phép lưu thông trong hệ thống mạng.

VACLs có thể áp dụng trong phạm vi mạng VLAN hoặc giữa các mạng VLAN với nhau. VACLs có đặc điểm như Router VACLs (RACLs) có thể loại bỏ, cho phép hay tái định hướng các gói tin.

Do các đặc điểm ưu việt trên đây, khi cấu hình triển khai hệ thống mạng LAN ảo trong hạ tầng mạng của mình, người quản trị có thể kết hợp them kỹ thuật này (VACLs) để giúp hệ thống của mình được bảo mật tốt hơn, bên cạnh đó tận dụng được tính năng sẵn có của thiết bị và làm giảm chi phí bảo mật hệ thống mạng.

TÀI LIỆU THAM KHẢO

1. Eric Vyncke, Christopher Paggen, (2012), *LAN Switch Security: What Hackers Know About Your Switches*, Cisco Press.
2. Sean-Philip Oriyano, (2017), *CEH v9: Certified Ethical Hacker Version 9 Study Guide*, Wiley Publishing Inc.
3. Andrew Lockhart, (2010), *Network Security Hacks*, O'Reilly Media.
4. James F. Kurose, (2012), *Computer Networking: A Top-Down Approach*, Kuroseross.
5. Diane Teare, (2015), *CCNP Routing and Switching*, Cisco Press.

SUMMARY

COMBINNING VLAN-ACCESS LIST TO ENHANCE VLAN SECURITY EFFICIENT

Le Hoang Hiep*, Pham Thi Lien
University of Information and Communication Technology - TNU

As the number of VLANs increases, the management of IP traffic which requires more basic level of security for network access becomes more difficult, then the network administrator have to need a technology can meet the requirements of network management as efficiency, cost, bandwidth, ... and manage also other VLANs better. VACLs are another good layer of security to help control who can talk to who, much like access control lists that are in firewalls and Routers, however the difference is VACLs operate at layer two of the OSI model. There could be situations where you have multiple hosts on the same LAN and want to block traffic from reaching certain hosts within that same network.

Keywords: *LAN, VLAN, Access List, VLAN-Access List, Vlan Access-map*

Ngày nhận bài: 11/4/2018; Ngày phản biện: 04/5/2018; Ngày duyệt đăng: 31/5/2018

* *Tel: 0984 666500; Email: lhhiep@ictu.edu.vn*