**Lab 3. LAN Security**

SV thực hiện và viết báo cáo mô tả, giải thích kết quả thực hiện cho các nội dung sau:

Các bài lab:

* Port security
* DHCP snooping
* ACL
* Firewall
* Snort – IDS
* Network Monitoring System

1. **Port Security** (1,0 điểm)

Bằng cách giới hạn và kiểm soát các thiết bị gắn vào Switch có thể hạn chế nhiều tấn công trong LAN như:

* Kẻ tấn công dùng công cụ để quét lấy hết IP từ DHCP server
* Kiểm soát các thiết bị người dùng cố định, các server kết nối đến Switch (tránh sự thay đổi tự do trong quá trình vận hành hệ thống)

#### Topology



#### Yêu cầu

1. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch (tùy vào PC, SV có thể dùng địa chỉ MAC khác).

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

3. port fa0/1 sẽ khôi phục lại sau 30 giây.

#### Cấu hình

1. Cấu hình port security. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch.

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

*(Switch(config-if)#switchport port-security mac-address 0040.4519.7183)*

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

Switch(config-if)#switchport port-security mac-address sticky

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

Switch(config)#interface fa0/1

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

3. port fa0/1 sẽ khôi phục lại sau 30 giây *(các lệnh sau không hỗ trợ trên phần mềm giả lập Packet Tracer, – SV không cần làm chức năng này hoặc thử nghiệm trên GNS3)*

Switch(config)#errdisable detect cause all

Switch(config)#errdisable recovery cause all

Switch(config)#errdisable recovery interval 30

#### Kiểm tra cấu hình

*show interface switchport*

*show port-security interface*

1. **DHCP snooping** (2,0 điểm)

Chống giả các DHCP server trong hệ thống, chỉ cho phép các client xin IP từ DHCP Server thật *(sử dụng phần mềm giả lập Packet Tracer hoặc EVE)*



#### Topology

Yêu cầu

1. Cấu hình theo sơ đồ mạng trên

* Cấu hình định tuyến
* Cấu hình cho DHCP server cấp phát địa chỉ IP động cho các PC ở các mạng 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24

1. Thử trường hợp với các DHCP server giả và AP cấp IP động
2. 2. Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server thật.

Các lệnh cấu hình:

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#no ipdhcp snooping information option

Switch(config)#interface <*interface*> (port kết nối hoặc port hướng kết nối về DHCP thật)

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit

#### Kiểm tra cấu hình

*show ip dhcp snooping*

*show ip dhcp snooping binding*

*show ip dhcp snooping database*

*show ip source binding*

1. **Access Control List** (2,0 điểm)

Cho sơ đồ mạng



Sử dụng lại bài Lab 01, có bổ sung thêm khu vực quản trị (Management zone)

1. Định tuyến cho khu vực Management Zone

Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2, Access-SW1 🡪 Access-SW6)

Trong đó:

* IP của các Acc-Sw1 🡪 Acc-SW3: 172.16.1.1/24 🡪 172.16.1.3/24
* IP của các Acc-Sw4 🡪 Acc-SW6: 172.16.2.4/24 🡪 172.16.2.6/24

1. Cấu hình ACL:

* Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server
* Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2, Access-SW1 🡪 Access-SW6)

1. **Firewall** (2,0 điểm)

* *ASA*
  + *Firewall rule: inside 🡪 outside*
* *Sinh viên tự chọn một Firewall dạng VMWare để thử nghiệm* ***(Fortigate****, Checkpoint,…)*

Topology



Thực hiện các rule:

* Cho phép các PC bên trong mạng nội bộ ra ngoài Internet
* Kiểm soát truy cập Web
* Kiểm soát port truy cập
* Kiểm soát ứng dụng truy cập
* Thực hiện các phương thức khác

SV có thể sử dụng các FW dạng VMWare: Fortigate, Checkpoint,…

1. **Snort-IDS** (2,0 điểm)



* Cài đặt Snort
* Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort

1. **Network Monitoring System** (1,0 điểm)

* Thực hiện giám sát mạng với phần mềm PRTG
* Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web,…), giám sát dung lượng đĩa trên Server
* Thiết lập ngưỡng cảnh báo

