**Lab 3. LAN Security**

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

1. **Port Security** (1,5 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)*

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** (1,5 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 DHCP Server.

DHCP Server1: Cấp dãy địa chỉ IP : 192.168.1.0/24

Defaul Gateway : 192.168.1.100

DNS: 8.8.8.8

DHCP Server2: Cấp dãy địa chỉ IP : 172.16.1.0/24

Defaul Gateway : 172.16.1.200

DNS: 172.16.1.200

2. Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server1.

Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server 1.

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#interface fa0/2 (nối với 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. **ACL (2 điểm)**

Topology:



**Yêu cầu:**

1. Cấu hình định tuyến cho hệ thống theo mô hình trên (làm trên PacketTracer)
2. Cấu hình ACL:
   1. Chỉ cho phép các PC thuộc mạng 172.16.10.0/24 truy cập tới Web server bằng dịch vụ Web (HTTP)
   2. Cấm PC thuộc mạng 172.16.20.0/24 ping tới FTP server (192.168.100.200)
   3. Chỉ cho phép máy Admin (172.16.10.10) telnet/SSH tới các router (R1, R2) và các Switch. *(SV có thể chọn làm với Telnet hoặc SSH)*
3. **Firewall** (2 điểm)

* *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** (1,5 điểm)



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

1. **Network Monitoring System** (1,5 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