|  |  |
| --- | --- |
| **Họ và tên**: Bùi Lê Thủy Tiên  **Mssv**: 22162048  **LAB 07**:  Network Infrastructure Sercurity  **Giảng viên**: TS. Huỳnh Nguyên Chính | **Nhận xét giáo viên** |

**Câu 1. Port Security**

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.

- Chuyển sang chế độ config bằng các câu lệnh

Switch> en

Switch# conf t

A black text on a white background

Description automatically generated

- Cấu hình port security

Switch(config)#interface fa0/1

🡪 cấu hình port fa0/1

Switch(config-if)#switchport mode access

🡪 cấu hình cổng fa0/1 thành cổng truy cập chỉ kết nối với 1 VLAN cụ thể mà chỉ định

Switch(config-if)#switchport port-security

🡪 bật tính năng port security

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

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

🡪 Xác định số lượng tối đa các địa chỉ MAC được phép truy cập qua cổng này. Trong trường hợp này, chỉ có một địa chỉ MAC được cho phép, vì vậy chỉ có một thiết bị có thể kết nối.

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

🡪 tính năng này cho phép switch tự động học địa chỉ MAC của thiết bị đầu tiên kết nối vào cổng và gán nó làm địa chỉ MAC được cho phép. Điều này giúp giảm công việc cấu hình bằng tay các địa chỉ MAC được phép trên cổng.

**\* Cấu hình dạng tĩnh**

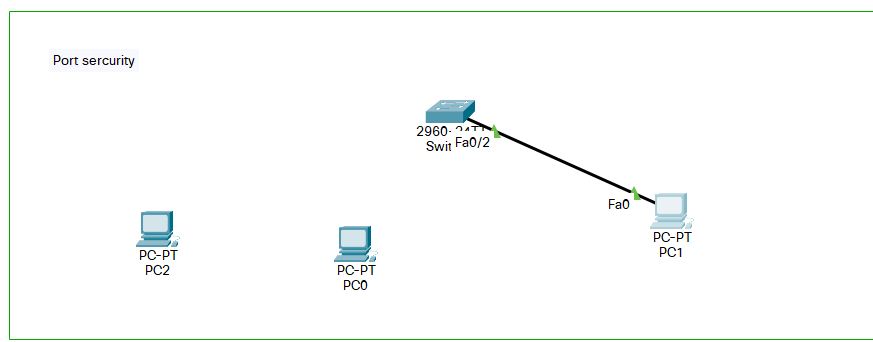
- Xem địa chỉ MAC của PC cần cấu hình Port sercurity

+ Địa chỉ MAC PC1:

**A screenshot of a computer

Description automatically generated**

**- Cấu hình Port sercurity:** Chỉ client có địa chỉ MAC là **000A.41B0.A268** được sự dụng port fa0/1 như mô hình

****

*Các câu lệnh cấu hình port sercurity tĩnh 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 maximum 1

Switch(config-if)#switchport port-security mac-address **000A.41B0.A268**

***- Các client khác khi kết nối với port fa0/1 sẽ bị shutdown***

Switch(config)#interface fa0/1

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

A computer code on a white background

Description automatically generated

- Kiểm tra hoạt động:

Tiến hành gắn PC0 vào port fa0/1, PC1 vào port fa0/2 như mô hình sau:

A computer network diagram with words

Description automatically generated

**Xem cấu hình:**

A screenshot of a computer program

Description automatically generated

**\* Cấu hình dạng động**

**- Xem địa chỉ MAC PC0:**

**A screenshot of a computer

Description automatically generated**

**- Cấu hình port sercurity:** PC0 với địa chỉ MAC là 000D.BD38.DD36 truy cập vô port fa0/1

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

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

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

A black text on a white background

Description automatically generated

- Sau cấu hình tiến hành thực hiện đặt IP và ping giữa 2 máy để tạo lưu lương cho switch học địa chỉ MAC

A screenshot of a computer program

Description automatically generated

- Sau đó vào switch kiểm tra xem đã học MAC của PC chưa bẳng lệnh

Switch> en

Switch# show run

A black text on a white background

Description automatically generated

A computer code with black text

Description automatically generated

**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

A white background with black text

Description automatically generated

- Ngắt kết nối với PC0 và cho PC2 kết nối vào port fa0/1 để kiểm tra, sau đó ping 2 máy

A diagram of a computer network

Description automatically generated

A screenshot of a computer

Description automatically generated

- Khi PC1 ping PC2 (hoặc bất kỳ thiết bị nào nằm trên cùng một mạng với PC2), switch sẽ nhìn thấy địa chỉ MAC của PC2 trong gói tin ping. Khi switch không tìm thấy địa chỉ MAC của PC2 trong bảng MAC của cổng fa0/1 và cổng này đã được cấu hình với max là 1 địa chỉ MAC, switch sẽ không học địa chỉ MAC của PC2 và cắt cổng (shutdown) để ngăn chặn tiềm ẩn cuộc tấn công từ một thiết bị không xác định

🡺 Ta dùng port security để quy định những máy nào có thể cắm vào port nào cụ thể.

#### Kiểm tra cấu hình

*show interface switchport*

*show port-security interface*

A screenshot of a computer

Description automatically generated

**Câu 2. DHCP snooping**

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

A diagram of a computer network

Description automatically generated

**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

DHCP Snooping có thể hiểu như một tính năng tường lửa bảo bật giúp ngăn chặn các cuộc tấn công của tin tặc vào hệ thống mạng của doanh nghiệp đánh cắp các thông tin quan trọng. Các tin tặng sẽ sử dụng các cách gửi các thông tin giẩ mạo để đánh lừa switch hay máy tính nhằm chuyển tiếp dữ liệu người dùng tới Getaway giả mạo. Mục đích chính của cá hacker tấn công là trở thành man in the middle, khi máy tính gửi dữ liệu đến gateway để ra mạng bên ngoài, hacker sẽ phân tích mọi thông tin dữ liệu chuyển tới vì máy tính của họ chính là cái Gateway giả mạo đó.

**Bước 1:**

Nhập địa chỉ IPv4: 192.168.1.254: **Server1 → Desktop → IPv4 Address**

A screenshot of a computer

Description automatically generated

Định cấu hình DHCP: **Server1 → Services** → **DHCP → On → Nhập thông tin → Save**

A screenshot of a computer

Description automatically generated

**Bước 2:**

Nhập địa chỉ IPv4: 192.168.1.200: **Server2 → Desktop → IPv4 Address**

A screenshot of a computer

Description automatically generated

Định cấu hình DHCP: **Server2 → Services** → **DHCP → On → Nhập thông tin → Save**

A screenshot of a computer

Description automatically generated

**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

A white background with black text

Description automatically generated

A white background with black text

Description automatically generated

- Vô PC3 lấy IP động chuyển tự static 🡪 dhcp, vào Desktop 🡪 IP configuration

A screenshot of a computer

Description automatically generated

#### Kiểm tra cấu hình

*show ip dhcp snooping*

A white screen with black text

Description automatically generated

*show ip dhcp snooping binding*

*A close-up of a document

Description automatically generated*

*show ip dhcp snooping database*

*A white screen with black text

Description automatically generated*

*show ip dhcp binding*

A black and white text

Description automatically generated

**Câu 3. Wifi Security**

1. **Cấu hình WiFi cơ bản**

* MAC filtering

A screenshot of a computer

Description automatically generated

* WPA2 – Personal

A screenshot of a computer

Description automatically generated

- Sơ đồ mạng:

A computer screen shot of a computer

Description automatically generated

* AP có IP 192.168.1.1/24

A screenshot of a computer

Description automatically generated

* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

**Yêu cầu:**

* ***Cấu hình AP – tên SSID SV tự cho***

A screenshot of a computer

Description automatically generated

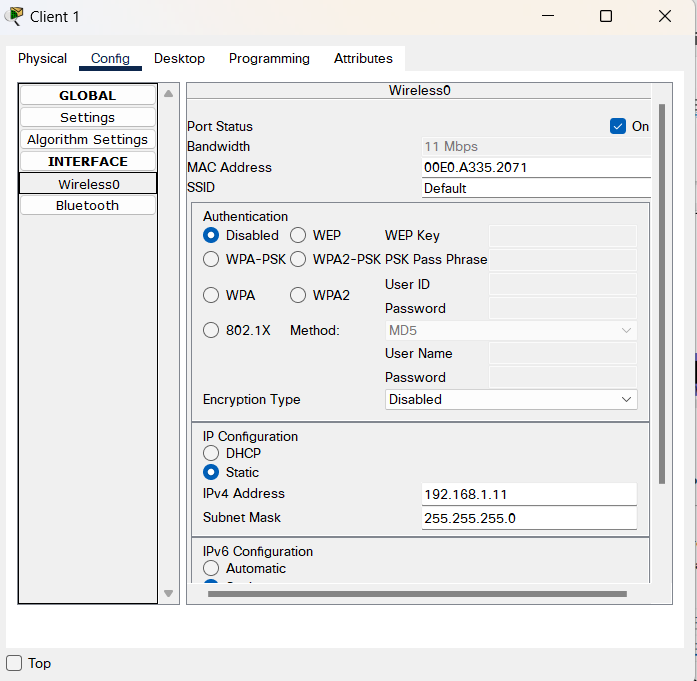
* ***Cấu hình AP làm DHCP server, các thông số IP cấp phát***
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8

A screenshot of a computer

Description automatically generated

* ***Cấu hình AP chỉ cho phép máy Client 1 và Client 2 sử dụng mạng WiFi (MAC filtering)***

+ *MAC Client 1*: 00.E0.E3.35.20.71. Cách kiểm tra địa chỉ MAC Client 1, tiến hành ấn vào laptop Client 1 ấn Config 🡪 Wireless và xem MAC



+ *MAC Client 2*: 00.D0.D3.5E.25.43. Cách kiểm tra địa chỉ MAC Client 2, tiến hành ấn vào laptop Client 2 ấn Config 🡪 Wireless và xem MAC

A screenshot of a computer

Description automatically generated

***- Cấu hình MAC filtering:*** Trong tab Wireless 🡪 Wireless MAC Filter bật enable và chọn lựa chọn Permit PC listed below to access wireless network, tức là cho phép các địa chỉ MAC dưới list truy cập được wifi

A screenshot of a computer

Description automatically generated

🡪 Như đã biết thì MAC address là địa chỉ độc nhất mà mỗi máy có do nhà sản xuất tạo ra, không máy nào có MAC giống máy nào. Vì vậy, MAC filtering là một ý tưởng rất hay trong việc phòng tránh crack password wifi, vì dù bên thứ ba có crack được pass wifi hay chính chúng ta đưa pass cho họ, thì họ cũng không thể truy cập được vào wifi này. Vì trong danh sách các địa chỉ MAC được cho phép không có máy họ.

A screenshot of a computer

Description automatically generated ***- Cấu hình WPA2-personal (password SV tự cho)***

A computer with a plug in

Description automatically generated with medium confidence***-*** Gắn card mạng để các client có thể kết nối wifi

***-*** Dùng máy Client 1 để connect vào wifi TienBui đã cấu hình cho phép máy laptop client 1 truy cập

A screenshot of a computer

Description automatically generated

- Nhập pass là builethuytien như đã cấu hình access point ở các bước trước

A screenshot of a computer

Description automatically generated

- Dùng máy Client 2 để connect vào wifi TienBui đã cấu hình cho phép máy laptop client 2 truy cập

A screenshot of a computer

Description automatically generated

- Nhập pass là builethuytien như đã cấu hình access point ở các bước trước

A screenshot of a computer

Description automatically generated

- Connect Client 3 sử dụng wifi nhưng không được vì không nằm trong dài các MAC cho phép khi cấu hình ở bước MAC filtering.

A screenshot of a computer

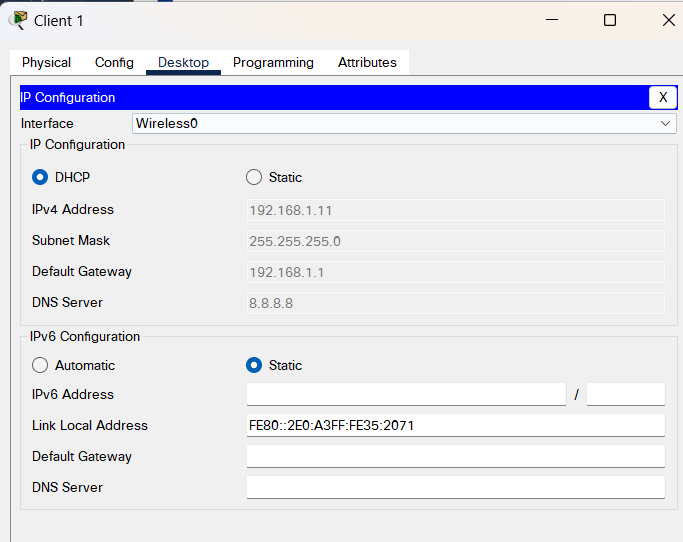
Description automatically generated

- Kết quả thu được sau khi cấu hình:

A computer screen shot of a computer

Description automatically generated

- Khi cấu hình ta đã cho access point cũng đóng vai trò là DHCP server, kiểm tra xem Client 1 đã được cấp phát chưa



- Đối với Client 2

A computer screen shot of a computer

Description automatically generated

- Đối với Client 3 do không thể kết nối tới access point nên yêu cầu cấp DHCP thất bại

A screenshot of a computer

Description automatically generated

1. **Cấu hình chứng thực người dùng WiFi dùng Radius Server**

A diagram of a computer network

Description automatically generated

* AP có IP 192.168.1.1/24

A screenshot of a computer

Description automatically generated

* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

**Yêu cầu:**

* ***Cấu hình AP – tên SSID SV tự cho***

A screenshot of a computer

Description automatically generated

- ***Cấu hình cho DHCP server***

+ Cấu hình IP tĩnh cho DHCP server

A screenshot of a computer

Description automatically generated

- Cấu hình bật chế độ dịch vụ DHCP trên server

A screenshot of a computer

Description automatically generated

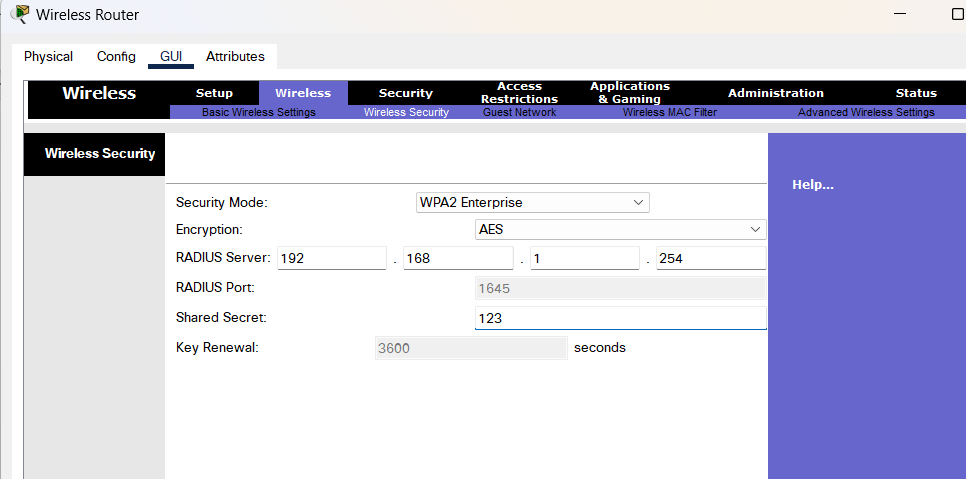
- Cấu hình Radius Server trên server

A screenshot of a computer

Description automatically generated

* ***Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi***

- AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)



* Authentication Server cũng đóng vai trò là DHCP server cấp pháp IP động cho các client trong mạng. Các thông số IP cấp phát như sau:
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8

- Kiểm tra IP đã cấp cho PC4

A screenshot of a computer

Description automatically generated

***- Cấu hình radius server trên access point***

Vào Desktop 🡪 PC Wireless 🡪 tab profiles ấn edit

A screenshot of a computer

Description automatically generated

Ấn advanced setup

A screenshot of a computer

Description automatically generated

Next tới đây chọn và chọn WPA2-Enterprise

A screenshot of a computer

Description automatically generated

- Username là ap và password là ap1 như đã cấp phát cho Radius server

A screen shot of a computer

Description automatically generated

Save and connect 🡪 thành công

A screenshot of a computer

Description automatically generated

Kết quả thu được sau cấu hình:

A diagram of a computer network

Description automatically generated

**Câu 3. Firewall**

* *Sinh viên tự chọn một Firewall dạng VMWare để thử nghiệm (Fortigate, Checkpoint,…)*

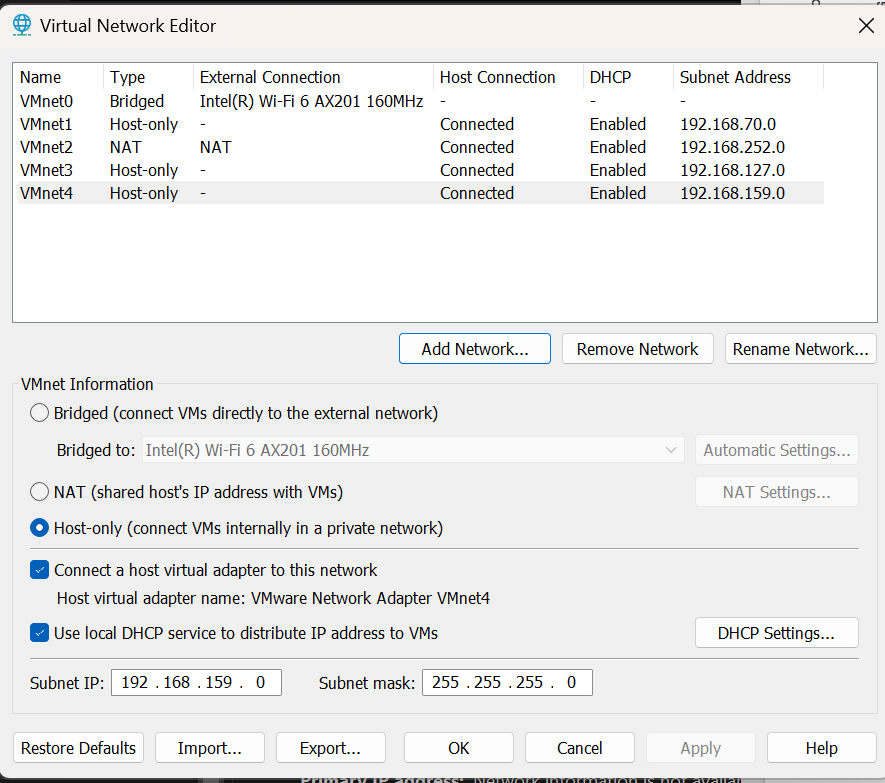
Topology



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,…  
- Cài đặt và cấu hình giao diện mạng ảo cho Vmnet3 và Vmnet4



- Cấu hình port netwrok

A screenshot of a computer

Description automatically generated

- Cấu hình giao diện quản lí

A screenshot of a computer program

Description automatically generated

- Cấu hình interface

A screenshot of a computer program

Description automatically generated

- Kết quả

A screenshot of a computer program

Description automatically generated

- Mở command prompt và test truy cập

A screenshot of a computer program

Description automatically generated

Truy cập vào địa chỉ IP đã nhập và login

A login screen with green and white squares

Description automatically generated

A screenshot of a computer

Description automatically generated

* Truy cập thành công

**Câu 4. Snort-IDS**



* Cài đặt Snort

+ Cài đặt snord bằng các câu lệnh sau đây

$ sudo apt update

$ sudo apt install snort -y

+ Sau đó kiểm tra snort đã cài đặt chưa

$ snort --version

A white paper with black text

Description automatically generated

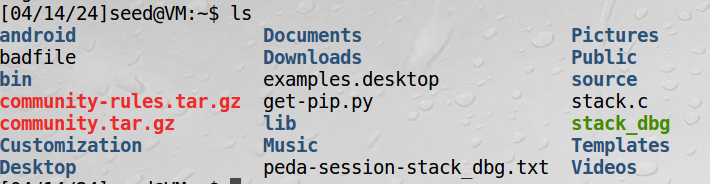
+ Tải thêm các rules của snort

$ wget https://www.snort.org/rules/community hoặc vào chrome tải

A close up of a computer screen

Description automatically generated

+ Tiến hành nhấn ls để xem tải về thành công chưa



+ Nếu đã thành công giải nén tệp tin bằng lệnh

$ sudo tar -xvf ~/communit-rules.tar.gz -C ~/

A screen shot of a computer

Description automatically generated

+ Copy toàn bộ thư mục vừa giải nén vào trong rules bằng lệnh:

sudo cp ~/community-rules/\* /etc/snort/rules

A screenshot of a computer screen

Description automatically generated

+ Chạy snort: sudo snort -T -c /etc/snort/snort.conf

A close up of a screen

Description automatically generated

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

+ Thêm rule phát hiện tấn công bằng ping, theo cú pháp sau

$ sudo vi /etc/snort/rules/local.rules

Thêm: alert icmp any any -> $HOME\_NET any (msg:”ICMP test”; sid:10000001; rev:001); vào file

A screenshot of a computer

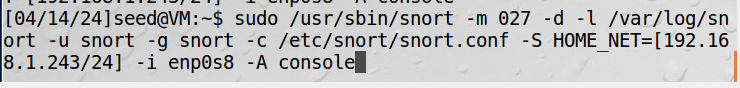
Description automatically generated

+ Thực thi snort: sudo /usr/sbin/snort -m 027 -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S HOME\_NET=[192.168.1.243/24] -i enp0s8 -A console

Với HOME\_NET là ip add máy

A screen shot of a computer

Description automatically generated



+ Máy attacker có IP nằm cùng mạng với máy sẽ ping tới máy

A screen shot of a computer

Description automatically generated

+ Sau đó phần mềm snort sẽ nhận diện được có máy lạ đang ping tới máy

A screenshot of a computer

Description automatically generated

+ Dùng nmap quét máy target

A computer screen shot of a computer program

Description automatically generated

+ Snort phát hiện báo có máy đang dùng nmap quét có ip là 192.168.1.17

A screen shot of a computer

Description automatically generated

+ Các thông tin về tag báo lên cảnh báo tấn công nằm trong scan.rules, có thể mở lên đọc tìm hiểu thêm

$ sudo vi /etc/snort/rules/scan.rules

A screen shot of a computer

Description automatically generated

🡪 Snort được sử dụng để phát hiện các hoạt động không mong muốn, tấn công mạng và các mẫu tấn công đã biết. Nó theo dõi lưu lượng mạng và so sánh với các quy tắc (rules) được xác định trước để nhận biết các hoạt động đáng ngờ hoặc nguy hiểm.

**Câu 5. Network Monitoring System**

* Thực hiện giám sát mạng với phần mềm PRTG

Tải và cài phần mểm PRTG

Cài đặt xong sẽ xuấ hiện giao diện sau:

A screenshot of a computer

Description automatically generated

* 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

Thêm thiết bị tiến hành giám sát, ấn Add Devices

A screenshot of a computer

Description automatically generated

Chọn thiết bị để quan sát, chọn printer (tùy ý)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Chọn Add sensor tring Overview phần Printers để thêm cảm biến

A screenshot of a computer

Description automatically generated

🡪 Beckhoff IPC System Health có thể theo dõi các thông số liên quan đến nhiệt độ, tài nguyên CPU, RAM, và các thông số khác

A screenshot of a computer

Description automatically generated

Thêm cảm biến thành công

A screenshot of a computer

Description automatically generated

* ***Thiết lập ngưỡng cảnh báo***

A screenshot of a computer

Description automatically generatedTa có thể theo dõi các giá trị performance trong giao diện quản trị PRTG. Nếu các giá trị vượt quá ngưỡng cảnh báo mà chúng ta đã thiết lập, PRTG sẽ gửi cảnh báo cho chúng ta.