Họ và tên: Lương Chin Du MSSV:21110870

Môn học: An toàn thông tin Mã môn: INSE330380\_23\_1\_09

Giảng viên hướng dẫn: Huỳnh Nguyên Chính

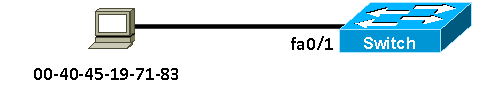
**Lab 7: Network Infrastructure Security**

**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: 0001.97EE.C06E được sử dụng port fa0/1 trên Switch (tùy vào PC, SV có thể dùng địa chỉ MAC khác).

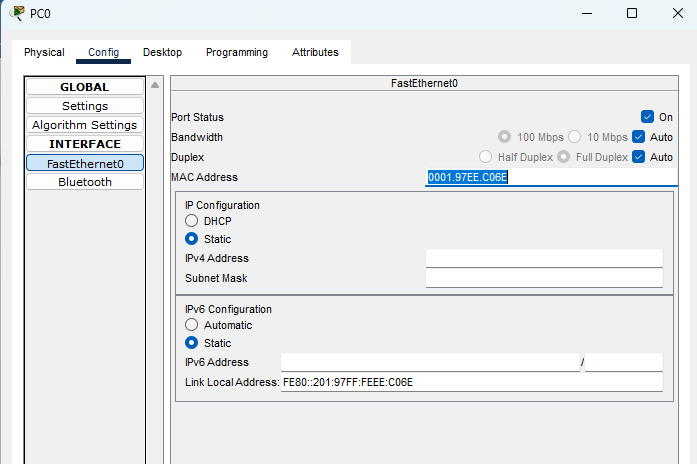
2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

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

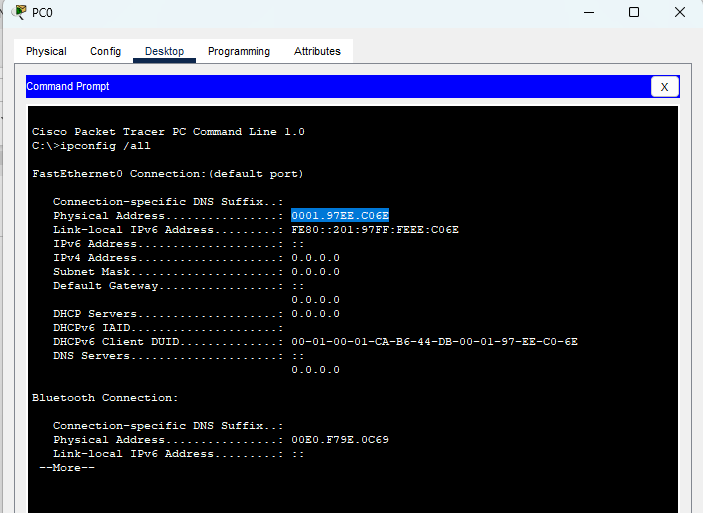
***Bước 1:***

**Xem địa chỉ MAC:**

Vào **Config → FastEthernet0**



Hoặc: **Desktop → Command Prompt và gõ lệnh ipconfig /all**



#### *Bước 2:*

#### *\* Cấu hình dạng tĩnh*

**1. Cấu hình port security. Chỉ có client với địa chỉ MAC:** 0001.97EE.C06E **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

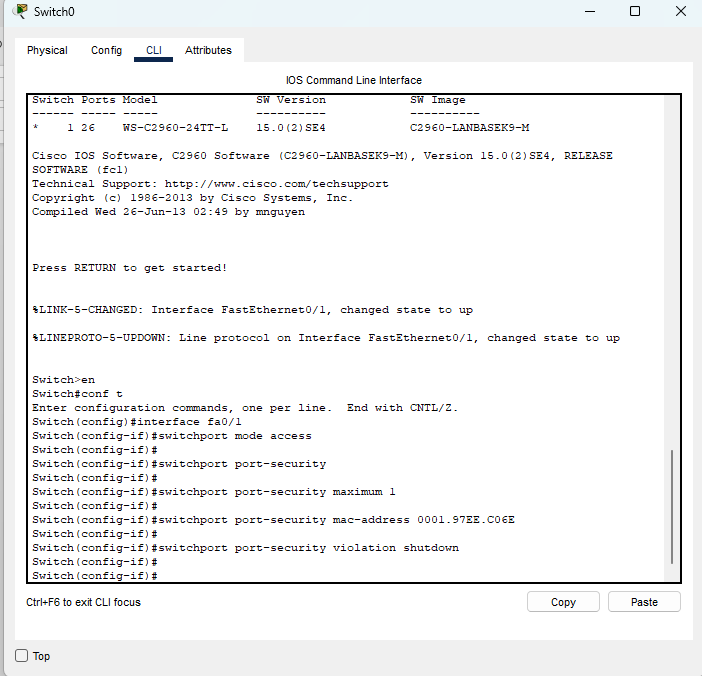
Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security mac-address 0001.97EE.C06E

**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



***\* Cấu hình dạng động:***

1. **Cấu hình port security**

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

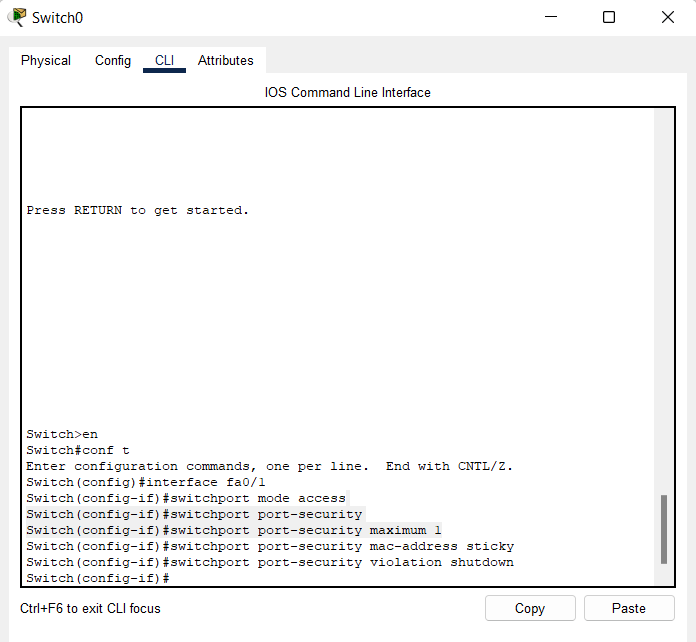
Switch(config-if)#switchport port-security maximum 1

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

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

Switch(config)#interface fa0/1

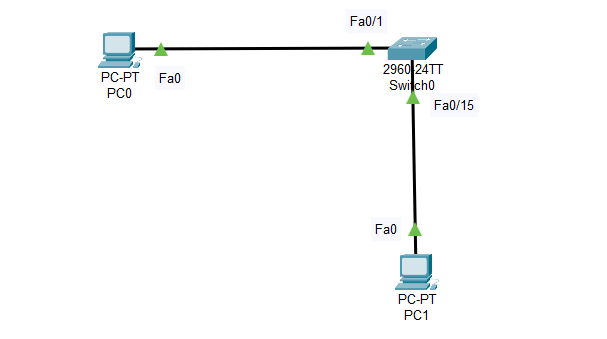
Switch(config-if)#switchport port-security violation shutdown



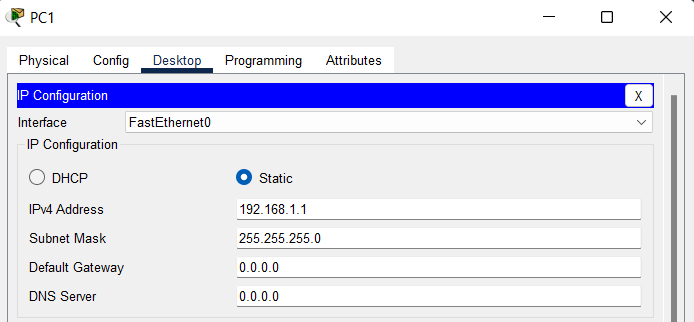
***Bước 3:***

***\* Cấu hình tĩnh:***

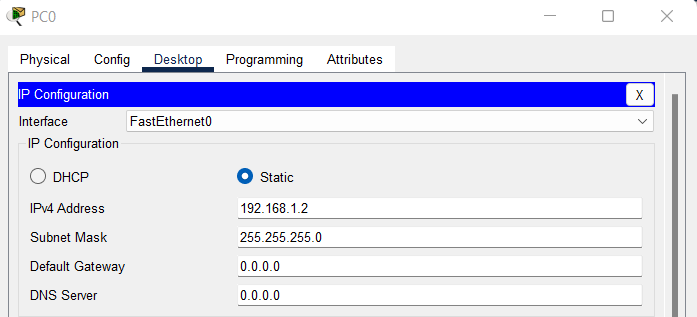
Lắp thêm một PC1 mới như sau:



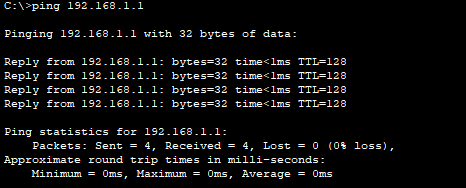
Đặt IP cho PC mới thêm vào (PC1): 192.168.1.1

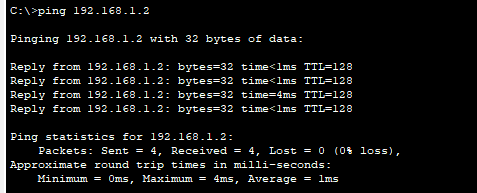


Đặt IP cho PC ban đầu (PC0): 192.168.1.2



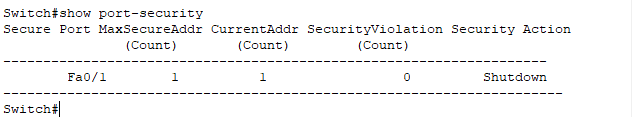
Ping giữa 2 máy:





Hoặc:

Dùng lệnh: **#show port-security**



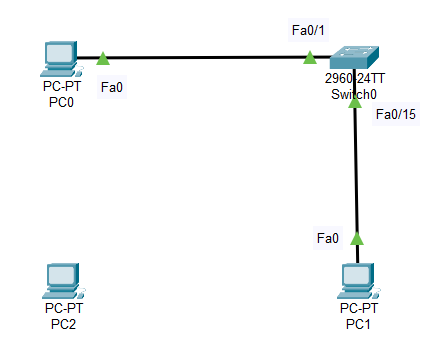
***\* Cấu hình động (tương tự)***

🡪 Ta thấy cấu hình: **Port Fa0/1,** chỉ cho một **(MaxSecurityAddr)** và một **(CurrentAddr)**, chưa thấy có máy vi phạm, nếu vi phạm thì sẽ **Shutdown** ngay.

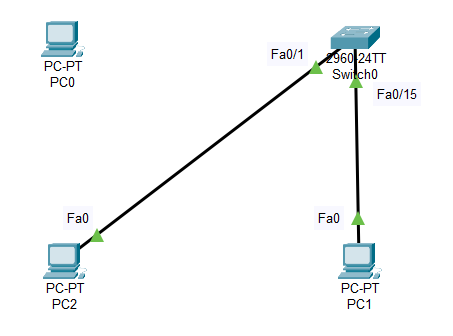
***Bước 4:***

**Giả sử:**

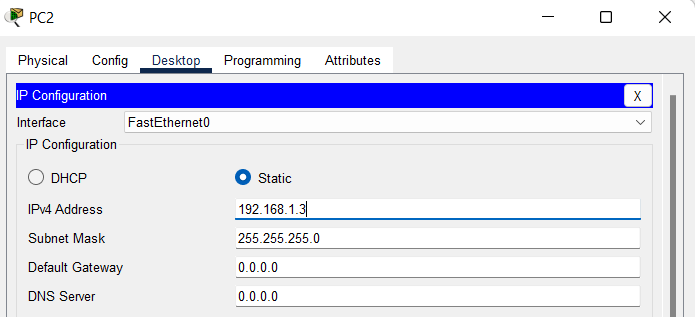
Lắp thêm một PC2:



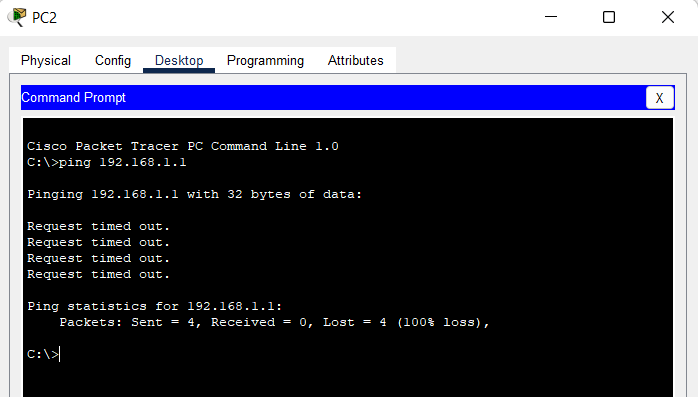
Gỡ bỏ dây kết nối giữa Switch0 - PC0, sau đó lắp dây vào Switch0 - PC2



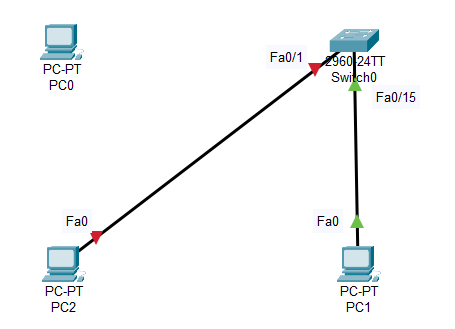
Đặt IP cho PC2: 192.168.1.3



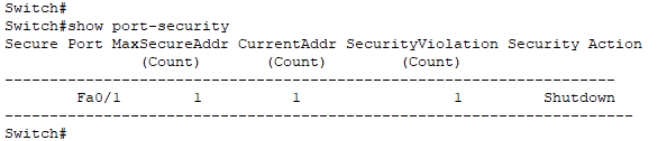
Sau đó: tiến hành ping đến máy PC1: 192.168.1.1



* Kết quả: Không thể ping được (do bị shutdown khi gắn vào cổng fa0/1 trên switch và không thể mở rộng mạng)



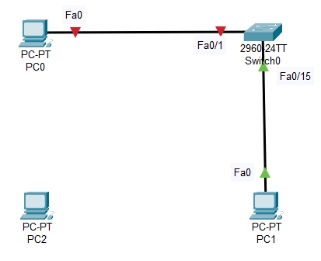
Dùng lệnh: **#show port-security** để kiếm tra



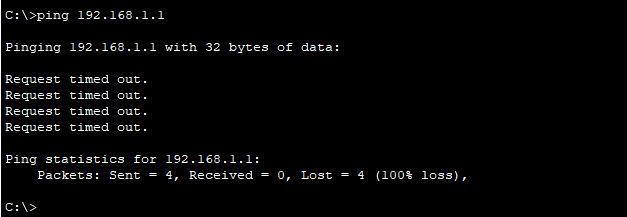
* Ta thấy rằng: có một máy bị vi phạm **(SecurityViolation) - bị Shutdown**

***Bước 5:***

Tiến hành tháo dây nối giữa Switch0 - PC2, gắn dây vào Switch - PC0



Ping lại PC 1 có Ip address 192.168.1.1

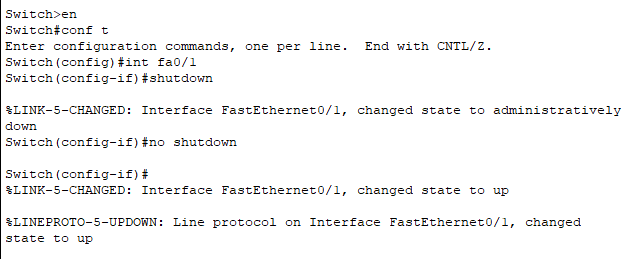


* Kết quả: vẫn không chạy được dù được gán IP: 192.168.1.2 (Block)

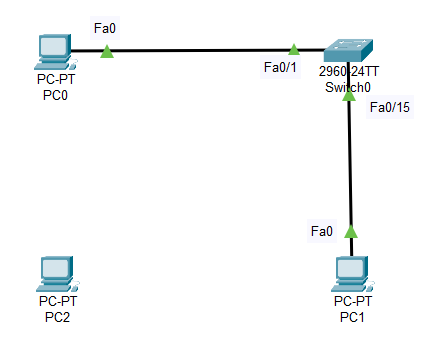
Để thực hiện kết nổi lại ta tiến hành các lệnh sau:

#shutdown

#no shutdown



* Kết quả: đã kết nối lại được switch.



**Quá trình chuyển trạng thái (port states):** được diễn ra theo trình tự

**Blocking → Listening → Learning → Forwarding**

Để chuyển trang thái nhanh hơn ta có thể dùng lệnh:

**#spaning-tree portfast default**



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)*

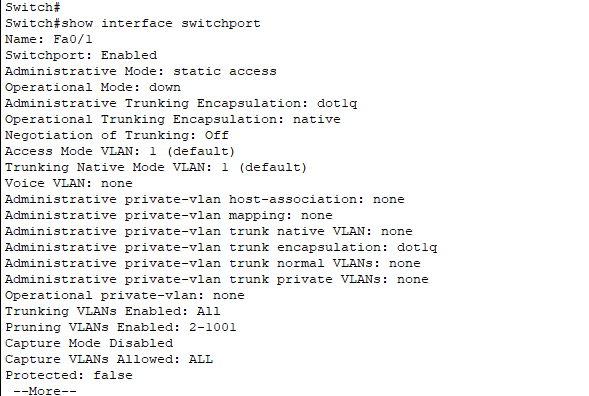
Switch(config)#errdisable detect cause all

Switch(config)#errdisable recovery cause all

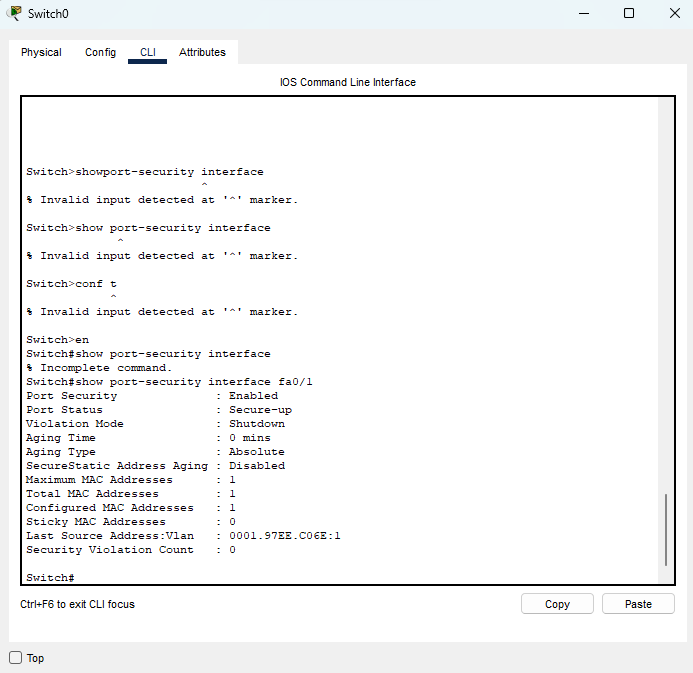
Switch(config)#errdisable recovery interval 30

#### Kiểm tra cấu hình

***show interface switchport***



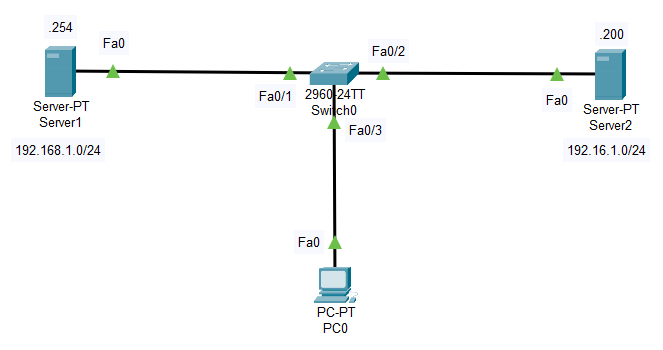
***show port-security interface***



**Câu 2. DHCP snooping (chống giả DHCP Serverse)**

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.**

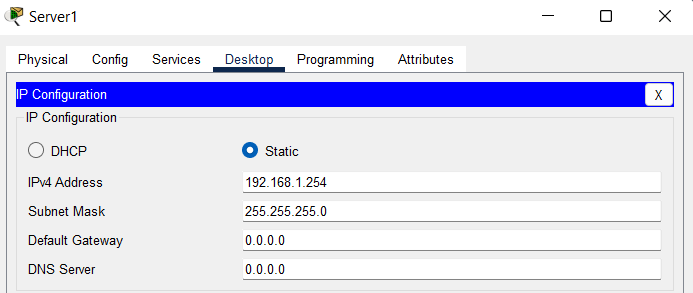
DHCP Server1: Cấp dãy địa chỉ IP: 192.168.1.0/24

Default Gateway: 192.168.1.100

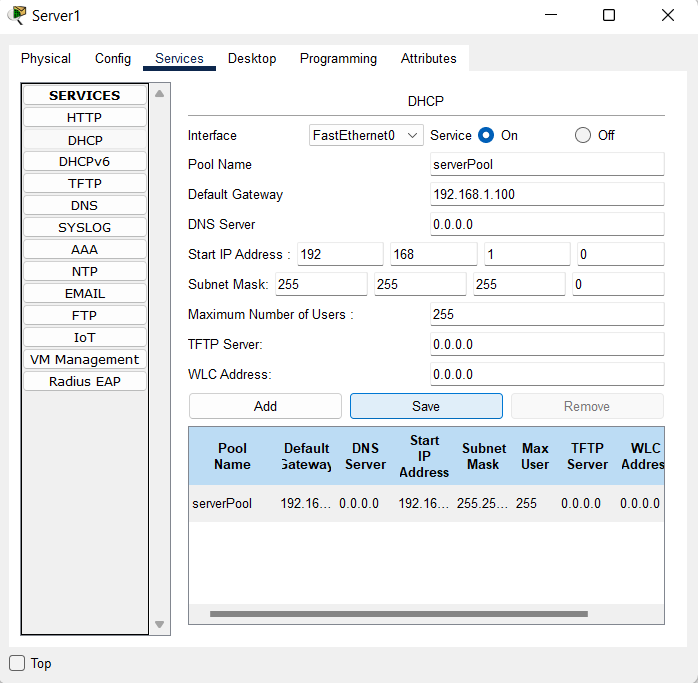
DNS: 8.8.8.8

**Bước 1:**

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



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



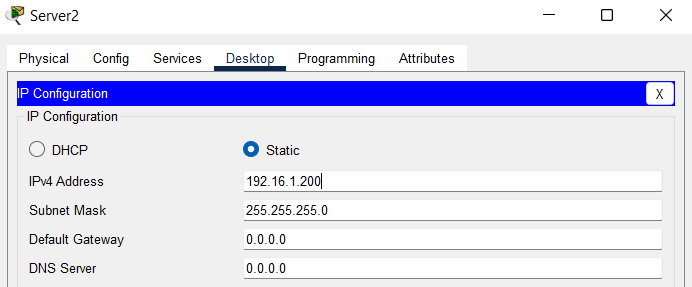
**Bước 2:**

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

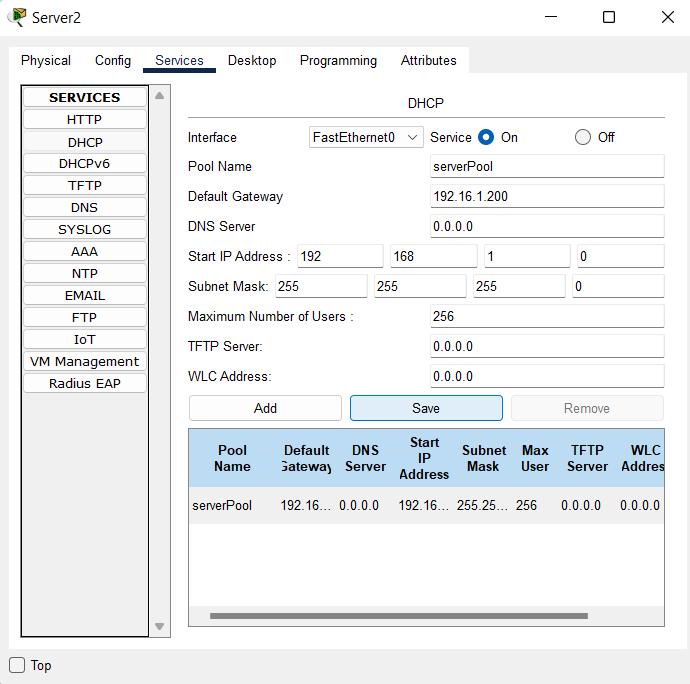
Defaul Gateway : 172.16.1.200

DNS: 172.16.1.200

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



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



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

**Bước 3:**

**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**

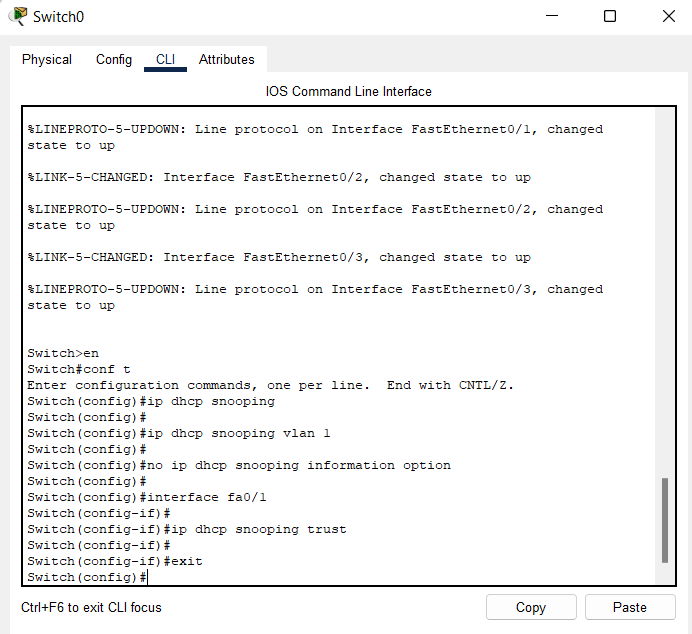
Switch(config)#**ip dhcp snooping vlan 1**

Switch(config)#**no ip dhcp snooping information option**

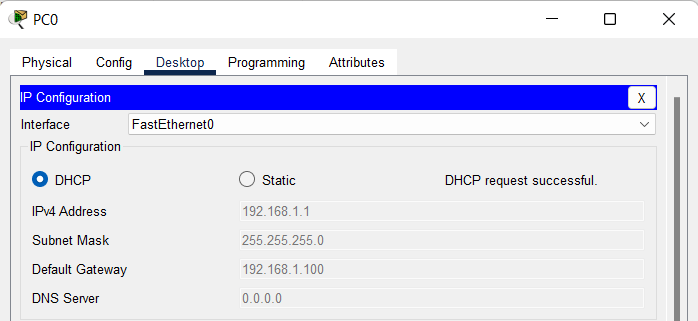
Switch(config)#**interface fa0/1 (nối với DHCP thật)**

Switch(config-if)#**ip dhcp snooping trust**

Switch(config-if)#**exit**



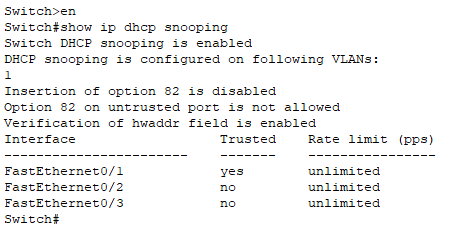
**Bước 4: Kiểm xem PC0 đang nhận địa chỉ DHCP IP từ Server nào : PC0 → Desktop → IP Configuaration → DHCP**



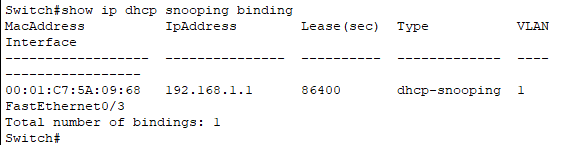
* Ta thấy rằng PC0 đang nhận địa chỉ DHCP IP từ Server1

#### Kiểm tra cấu hình

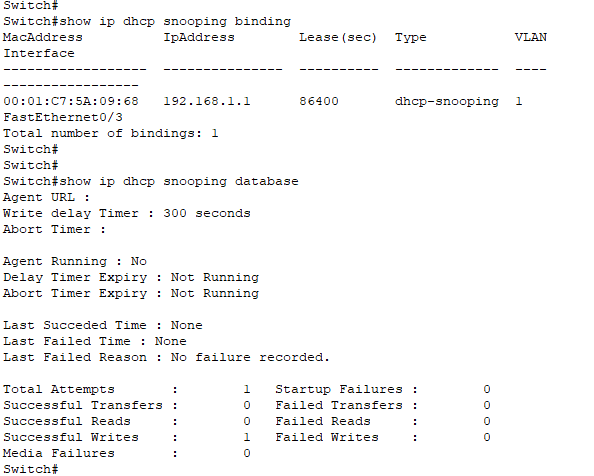
***show ip dhcp snooping***



***show ip dhcp snooping binding***



***show ip dhcp snooping database***



***show ip dhcp binding***

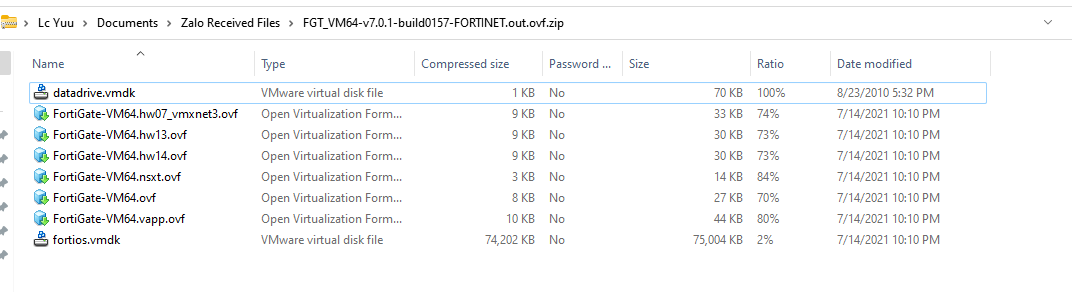


**Câu 3. Firewall**

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

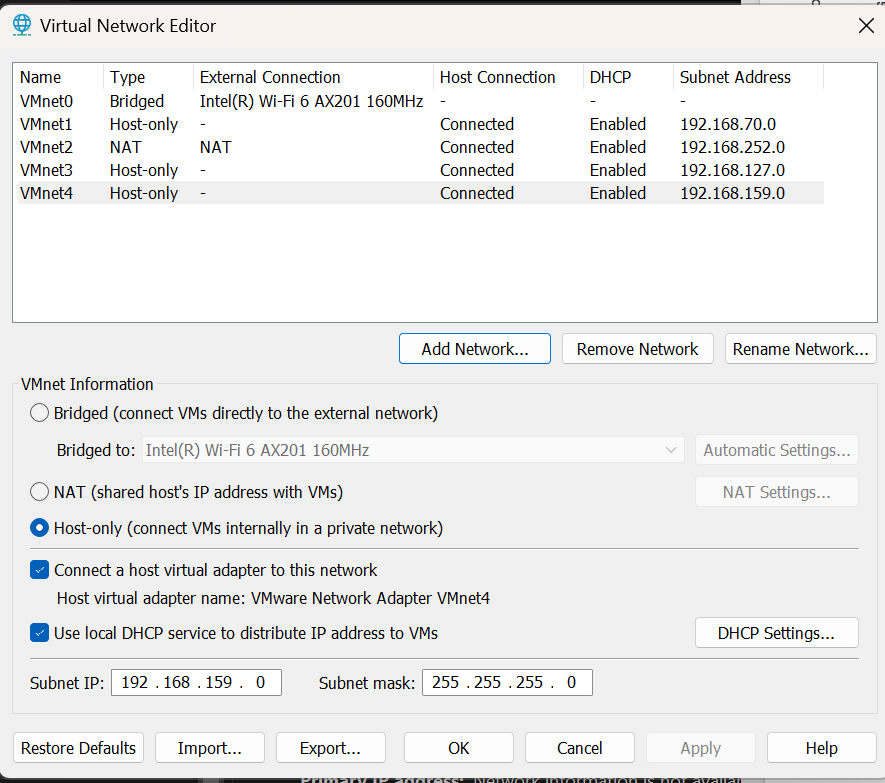
Cài đặt fortigate firewall

Download FortiGate Virtual firewall

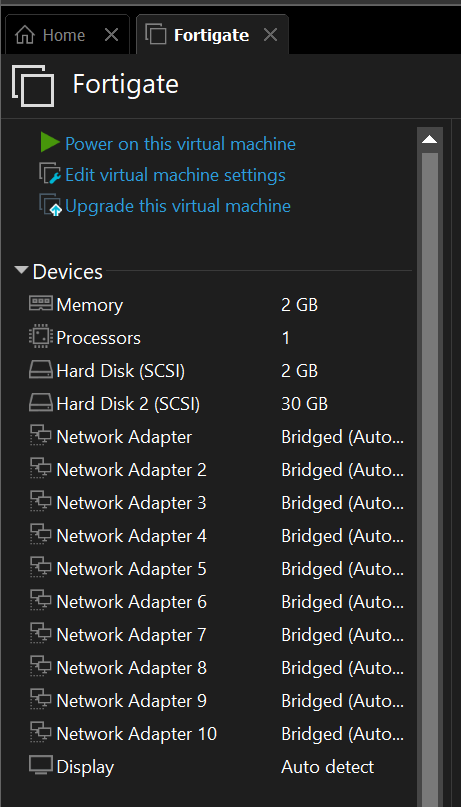


Định cấu hình giao diện mạng ảo cho FortiGate

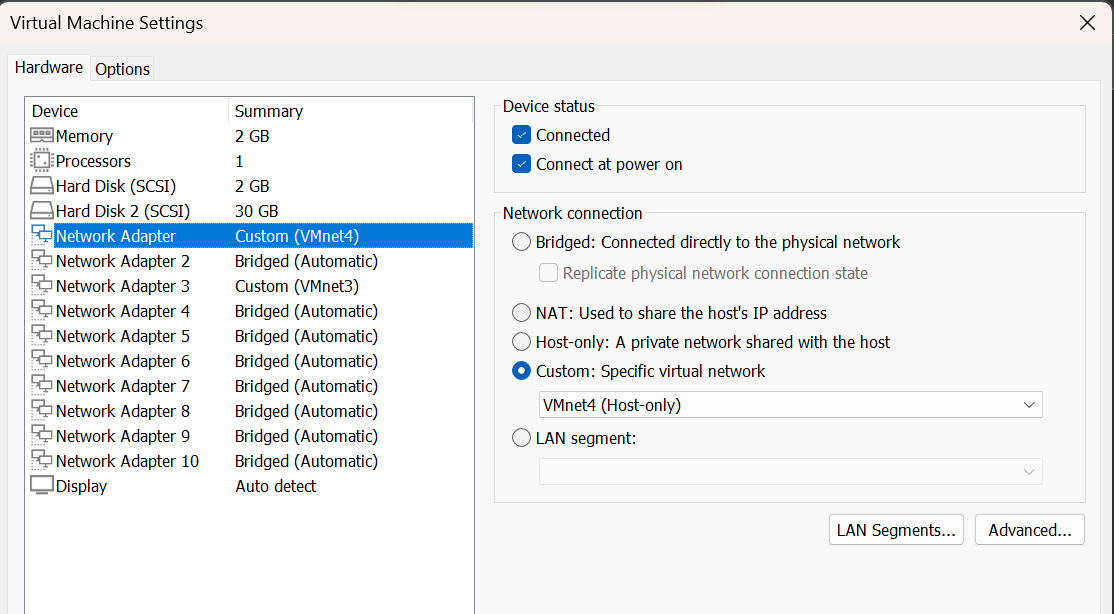
* Tạo mạng ảo cho VMnet3 và VMnet4



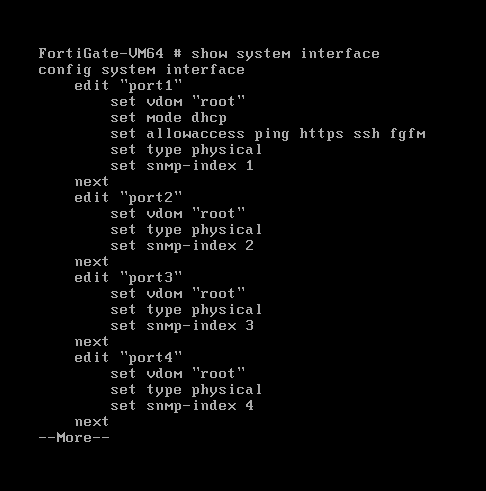
Nhập VM từ nguồn đã tải



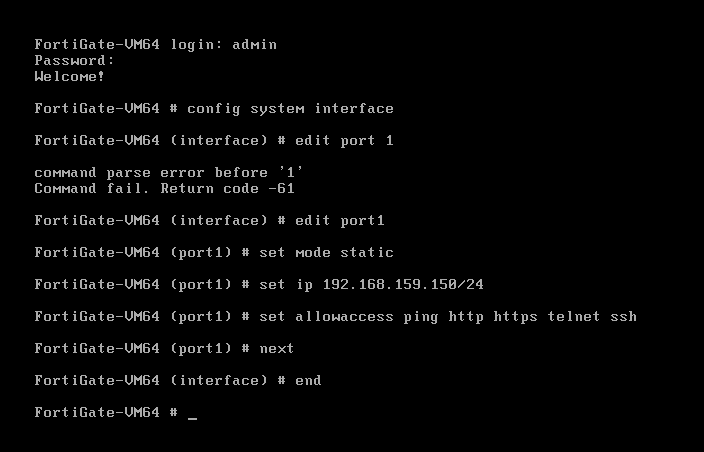
Cấu hình lại port network



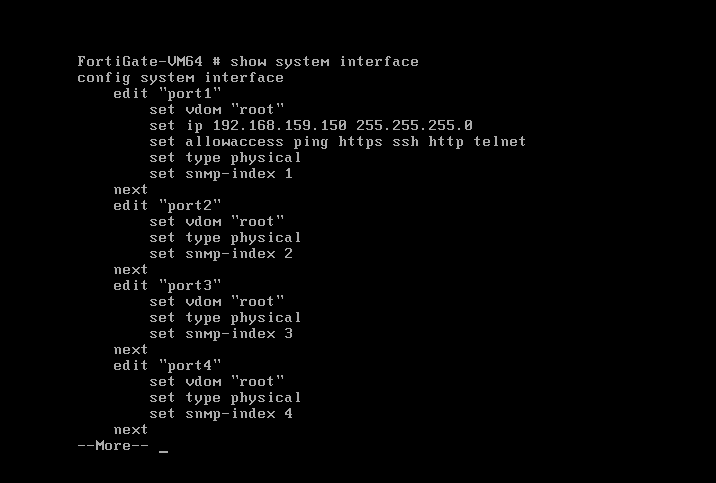
Định cấu hình giao diện quản lý



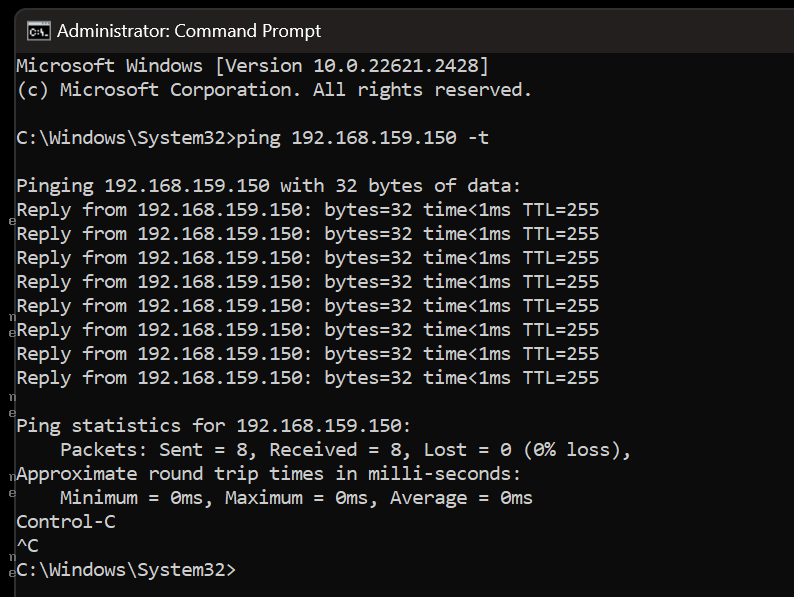
Config interface



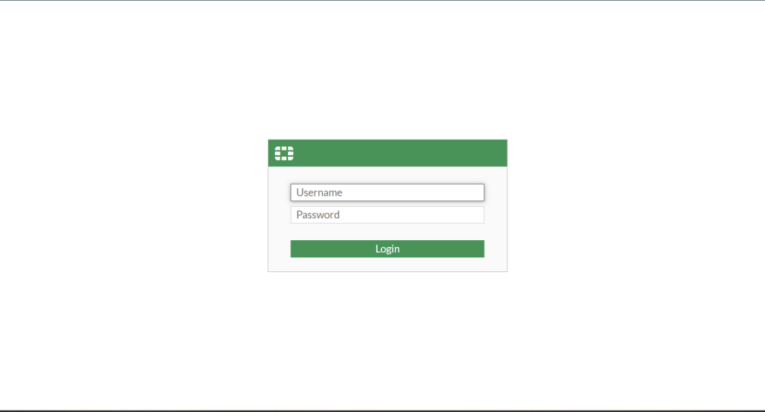
Kết quả:

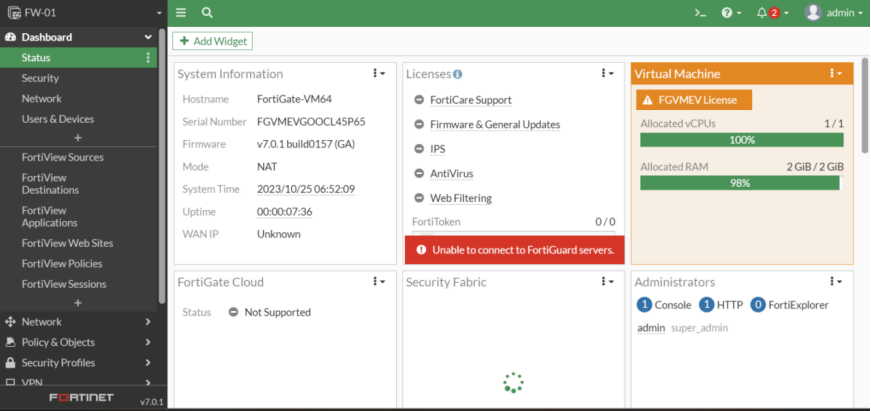


Mở cmd và test truy cập



Truy cập vào địa chỉ IP đã nhập và login





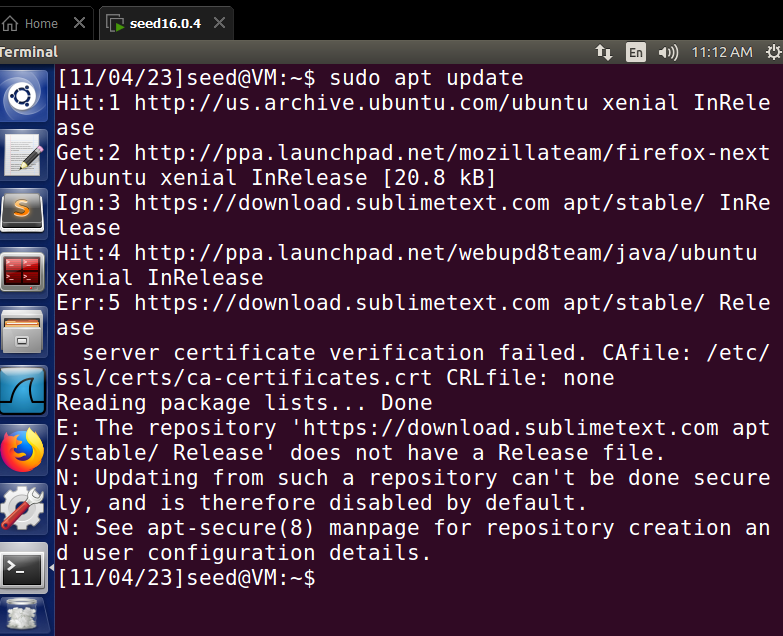
* Truy cập thành công

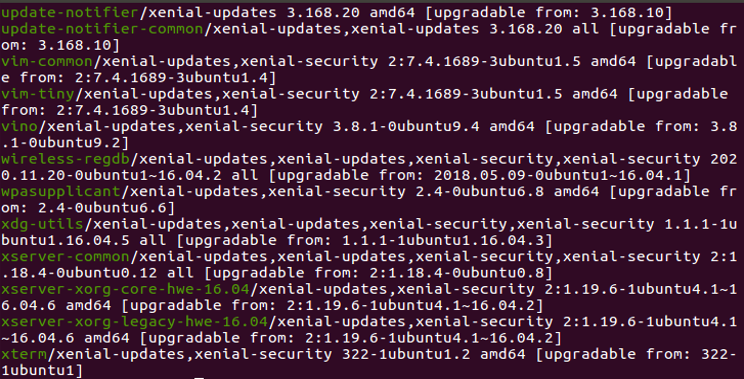
**Câu 4. Snort-IDS**



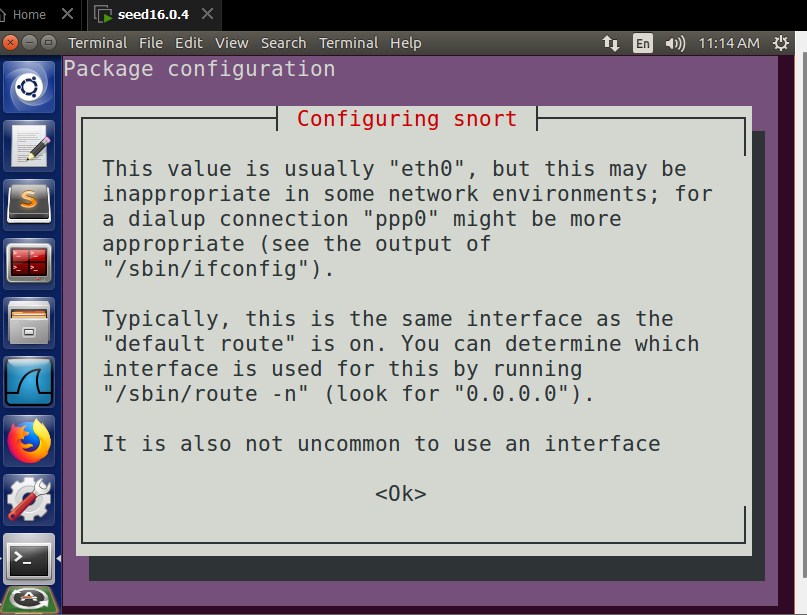
* Cài đặt Snort
* Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort
* Cài đặt Snort cho Seedubuntu:

Sudo apt update



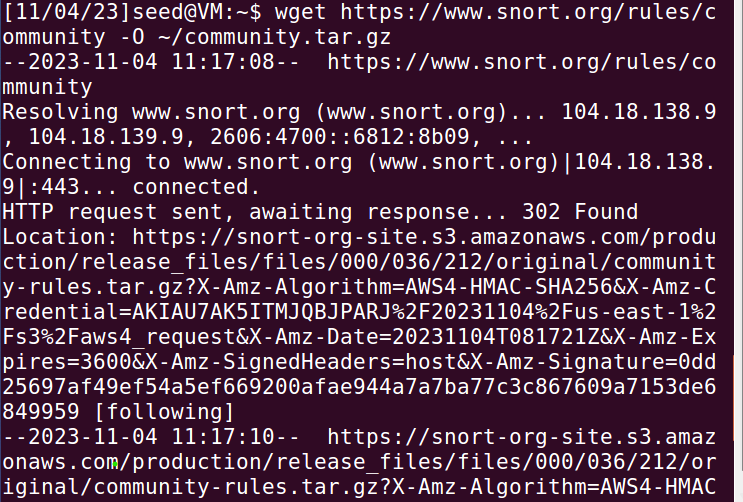


**Sudo apt install snort –y**

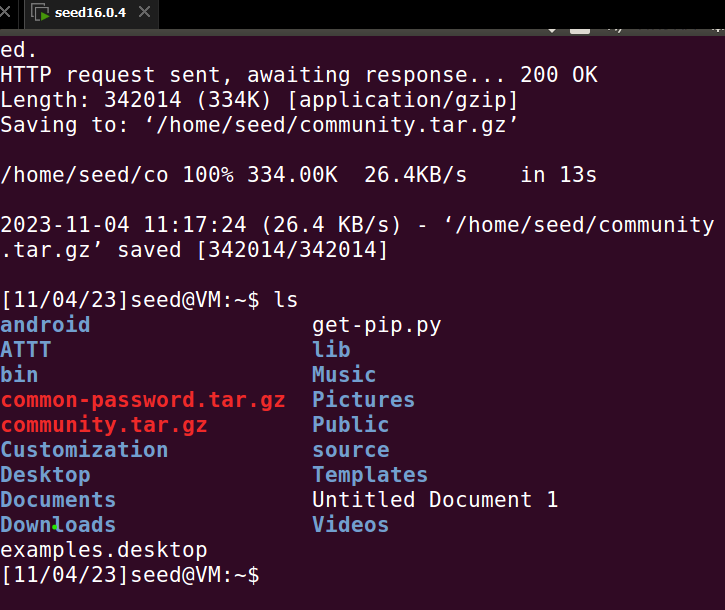


Tải và thêm các rules của Snort

wget [https://www.snort.org/rules/community -O ~/community.tar.gz](https://www.snort.org/rules/community%20-O%20~/community.tar.gz)

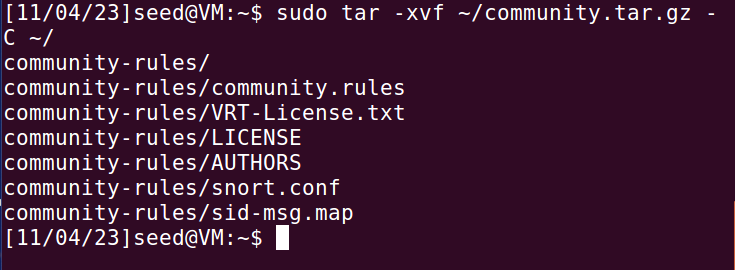


Lúc này ta sẽ có tập tin nén community.tar.gz chứa rules mà đã download

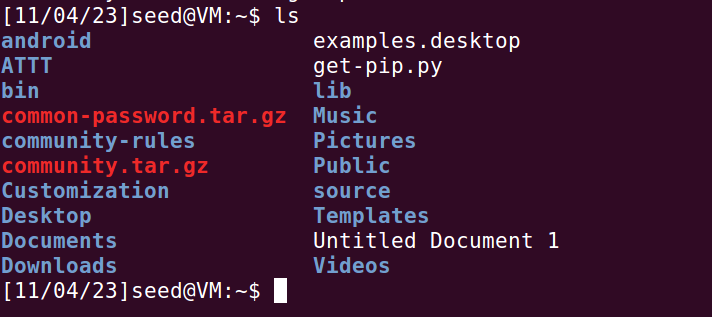


Sau đó giải nén tập tin bằng lệnh:

sudo tar –xvf ~/community.tar.gz –C ~/

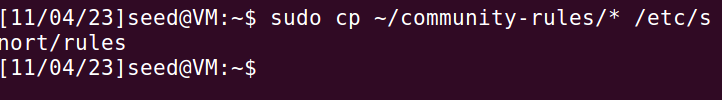


Lúc này tệp tin đã được giải nén là thư mục community-rules



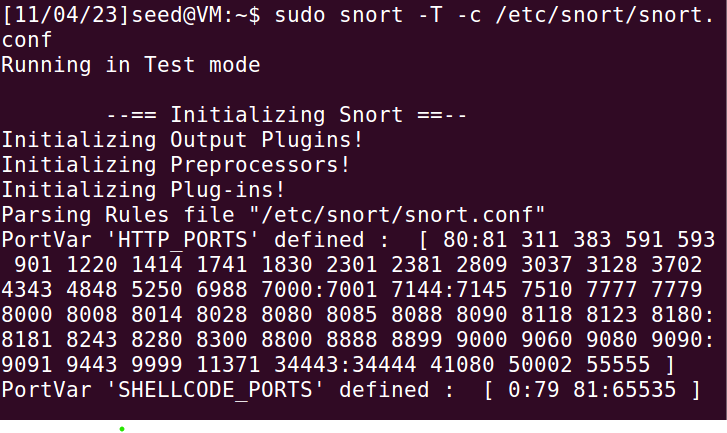
Copy toàn bộ thư mục vừa giải nén vào trong rules bằng lệnh:

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

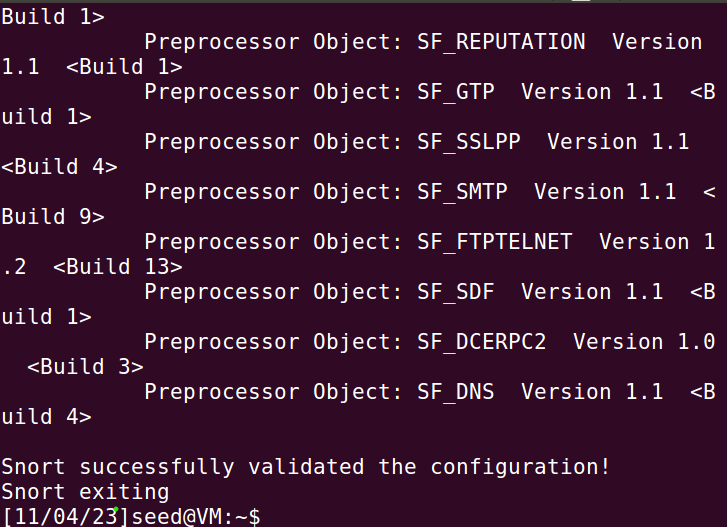


Chạy thử snort :

sudo snort –T –c /etc/snort/snort.conf



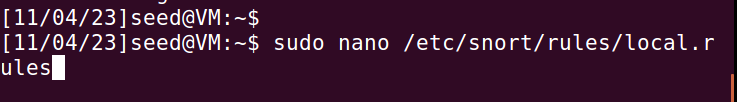
Cuối cùng đã cài đặt snort thành công



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

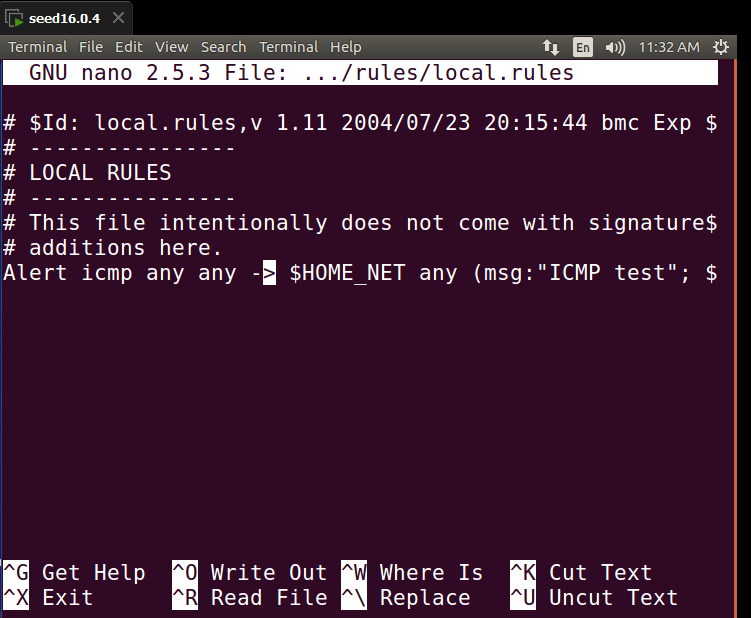
Thêm rules phát hiện tấn công bằng lệnh ping:

**Sudo nano /etc/snort/rules/local.rules**



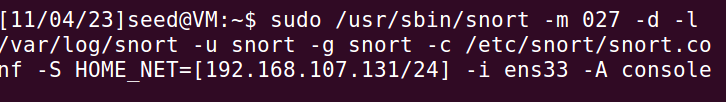
Thêm dòng sau:

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

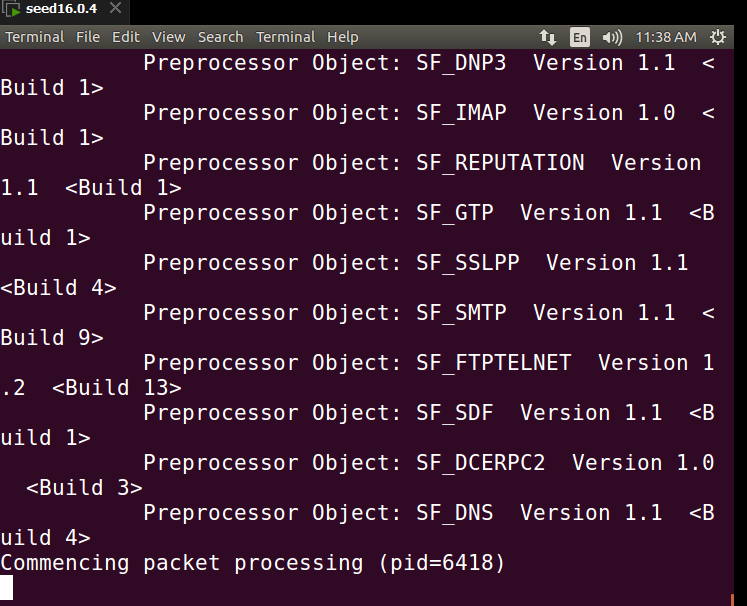


Thực thi snort:

sudo /usr/sbin/snort -m 027 -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S HOME\_NET=[192.168.107.131/24] -i ens33 -A console

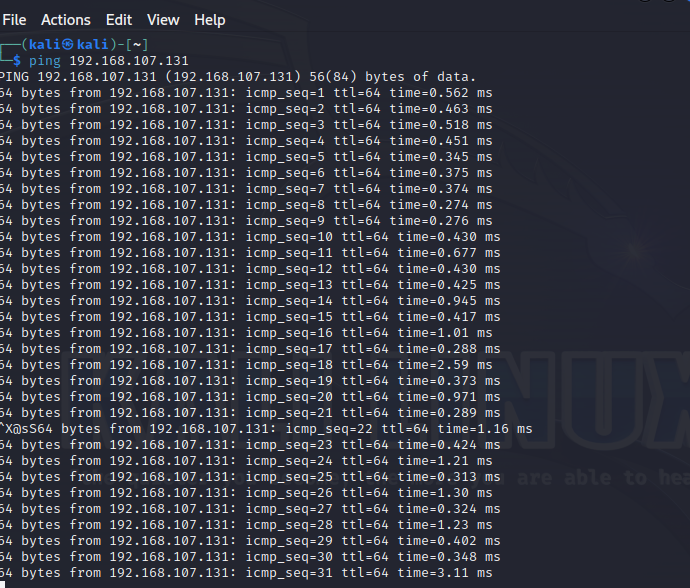


Lúc này công cụ snort đang hoạt động:

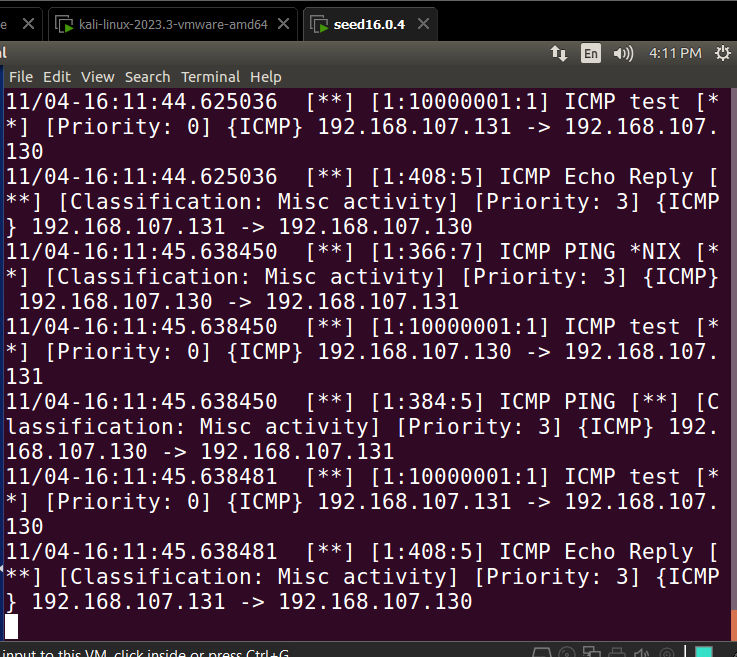


Trên máy kali thực hiện ping tới máy ubuntu:

ping 192.168.107.131

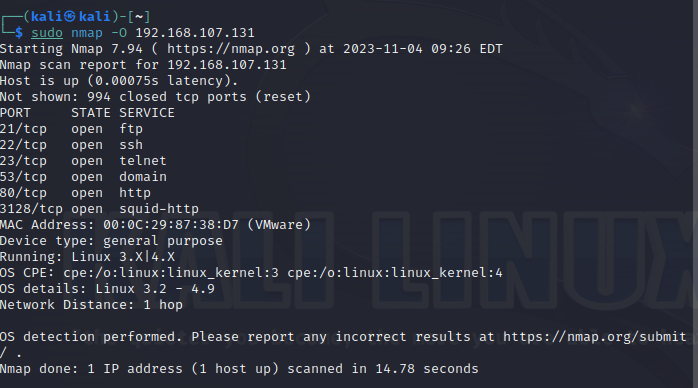


Lúc này snort đã chỉ ra các cảnh báo có lệnh ping thực hiện từ địa chỉ 192.168.107.130(địa chỉ IP máy kali) tới địa chỉ 192.168.107.131

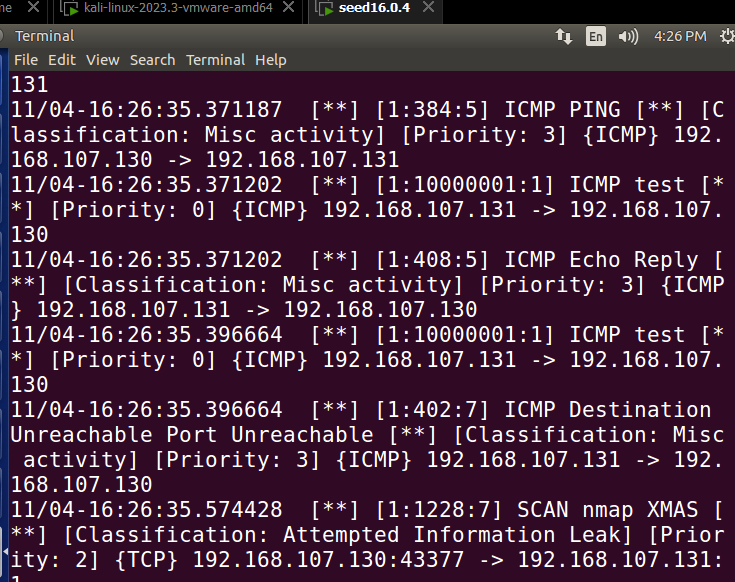


Trên máy kali sử dụng Nmap để quét máy ubuntu:

Sudo nmap -O 192.168.107.131



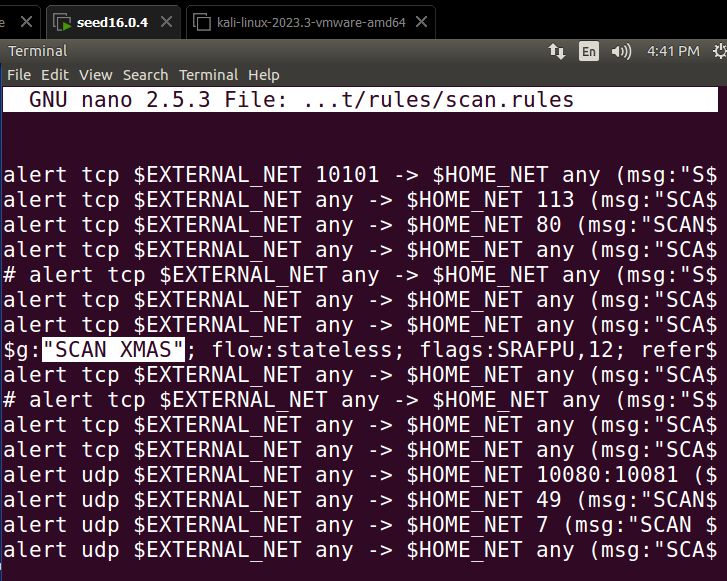
Trên máy ubuntu có xuất hiện thông điệp cảnh báo hiện nay có máy đang tấn công dạng quét cổng dùng Nmap tấn công dạng XMAS, máy tấn công có địa chỉ ip 192.168.107.130



Trên máy ubuntu phải có rules xuất hiện cảnh báo về log về sự tấn công trên, nằm trong scan.rules

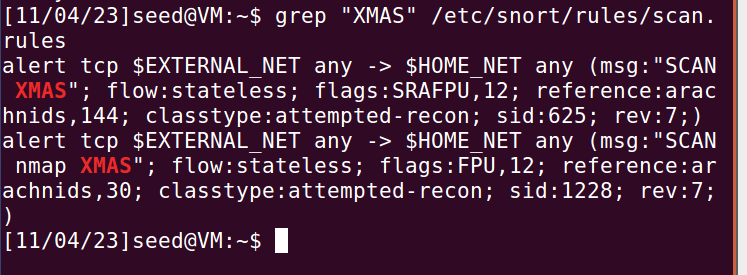


Trong đây sẽ có rất nhiều rules



Sử dụng lệnh tìm kiếm để thấy rules dễ hơn

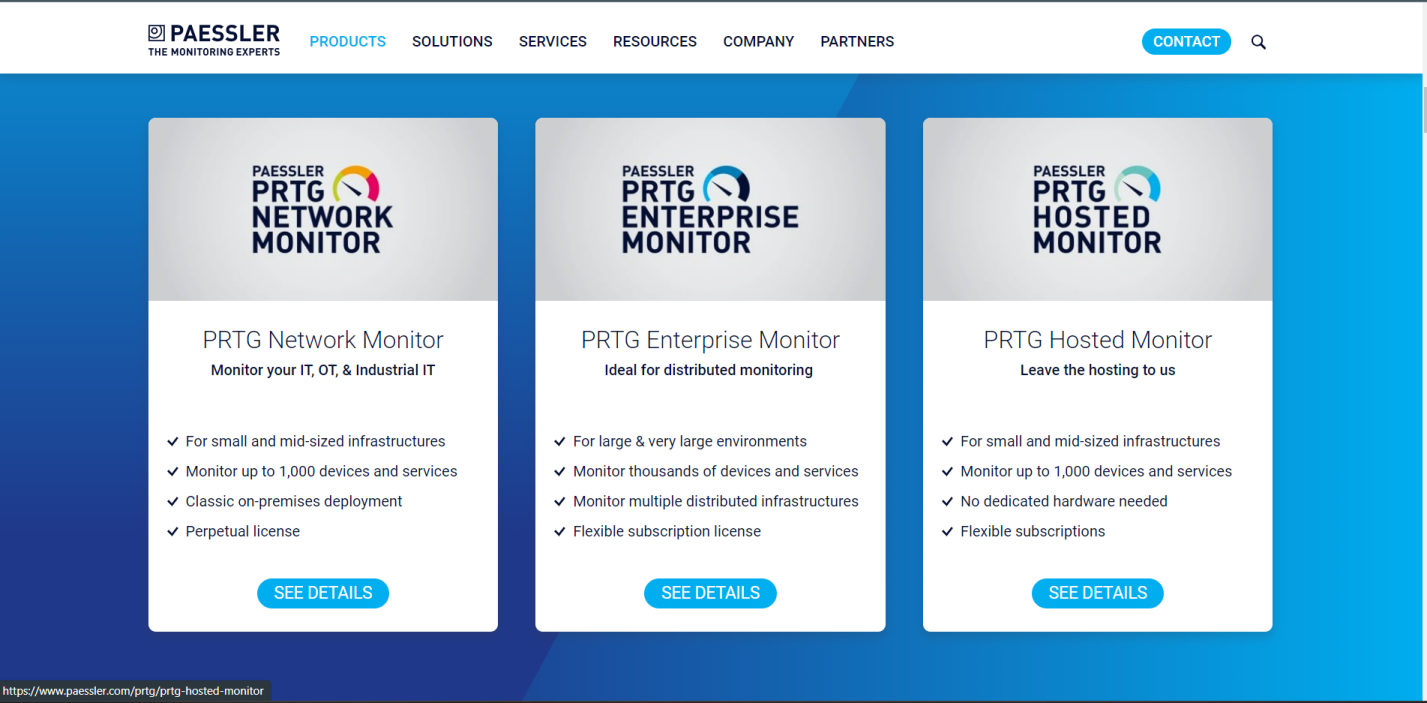
grep “XMAP” /etc/snort/rules/scan.rules

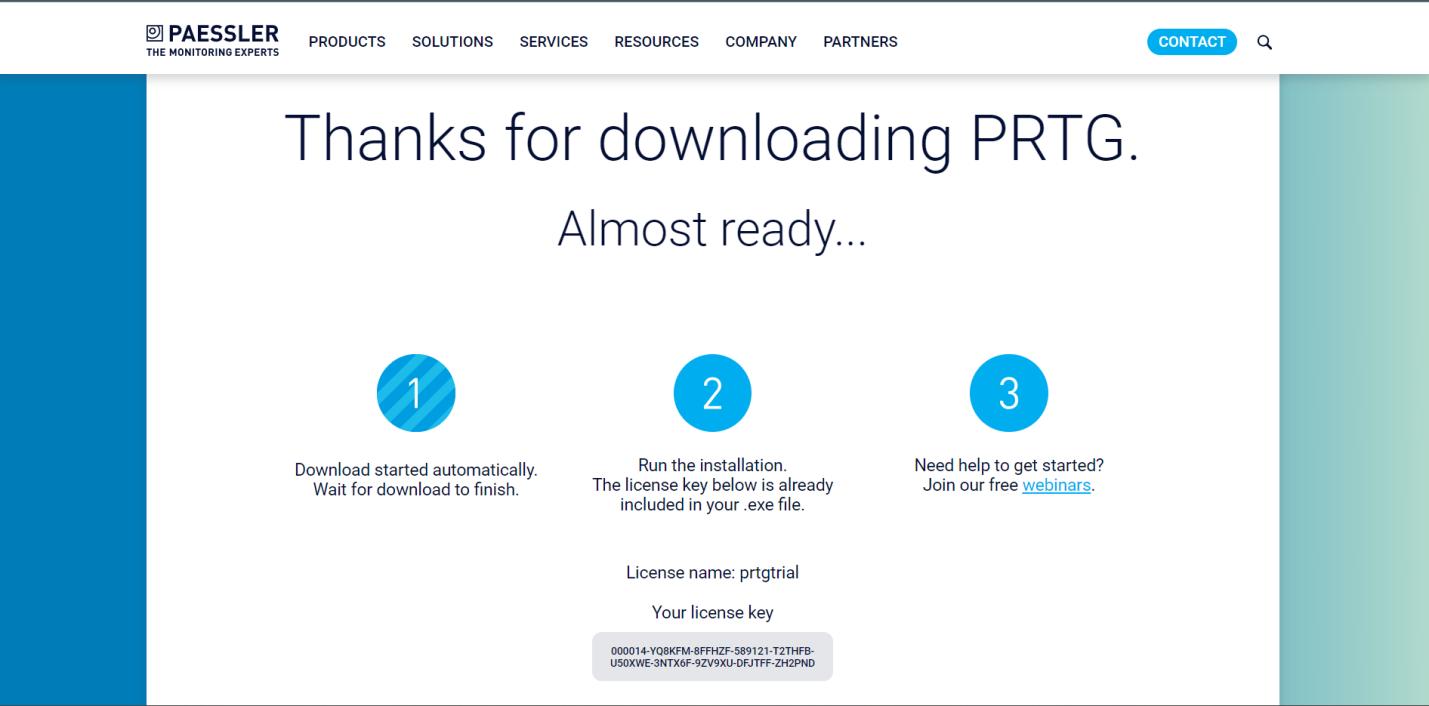


**Câu 5. Network Monitoring System**

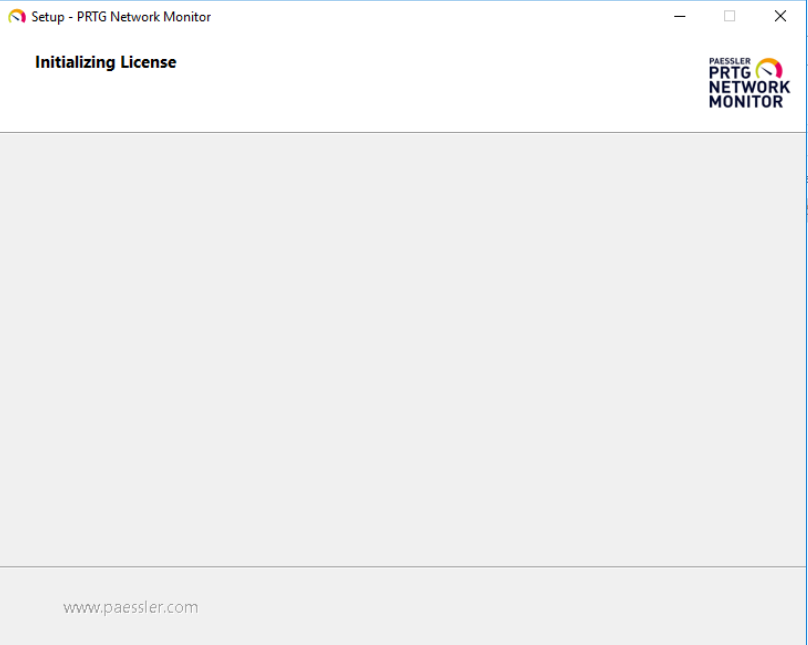
* Thực hiện giám sát mạng với phần mềm PRTG
* Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web…), giám sát dung lượng đĩa trên Server
* Thiết lập ngưỡng cảnh báo

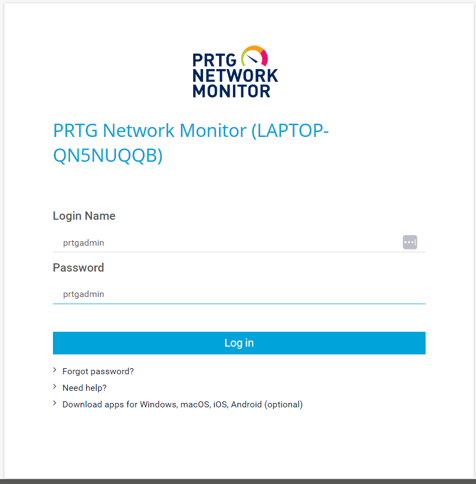
Download PRTG





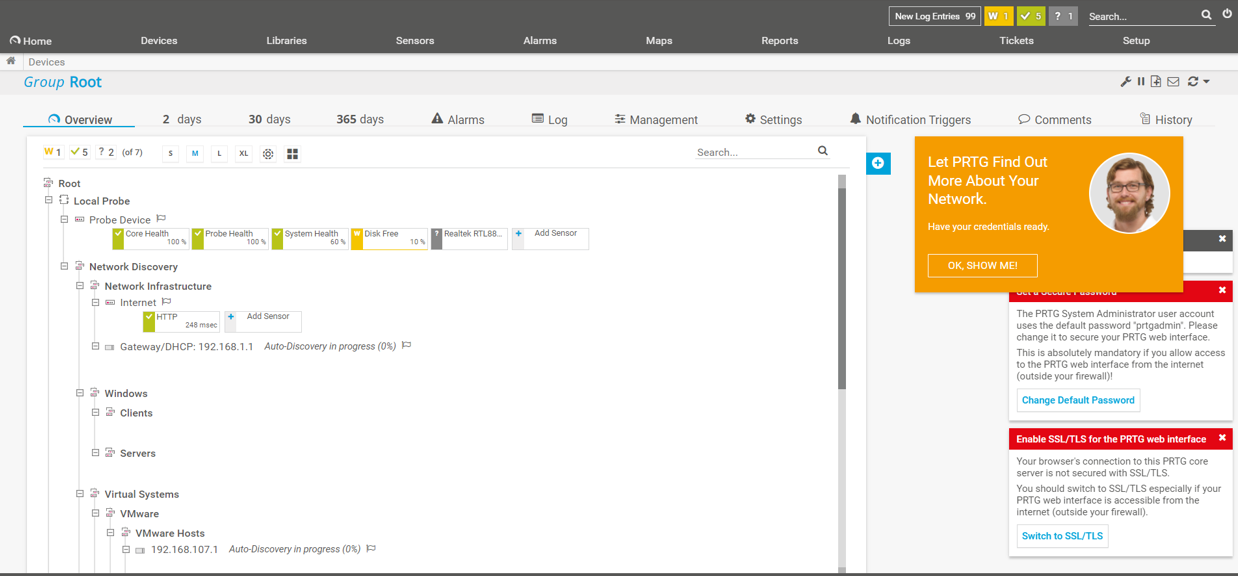
Cài đặt



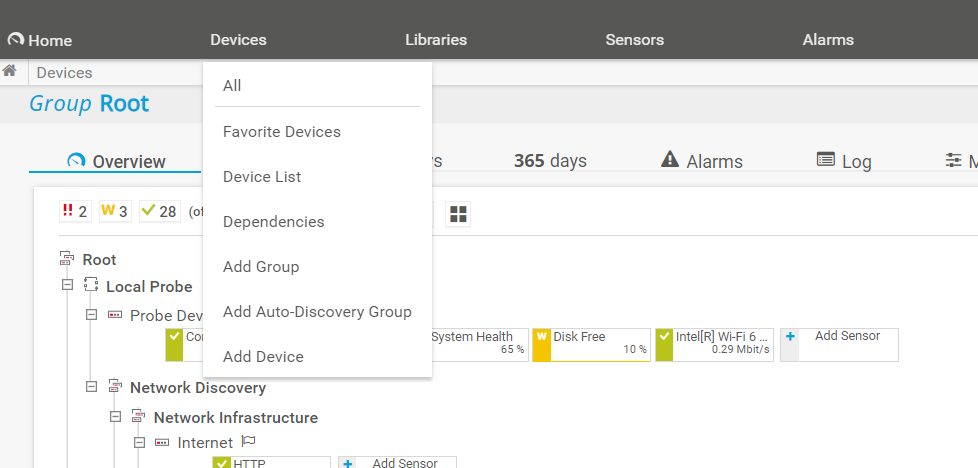


Sau khi cài đặt sẽ xuất hiện giao diện web của PRTG

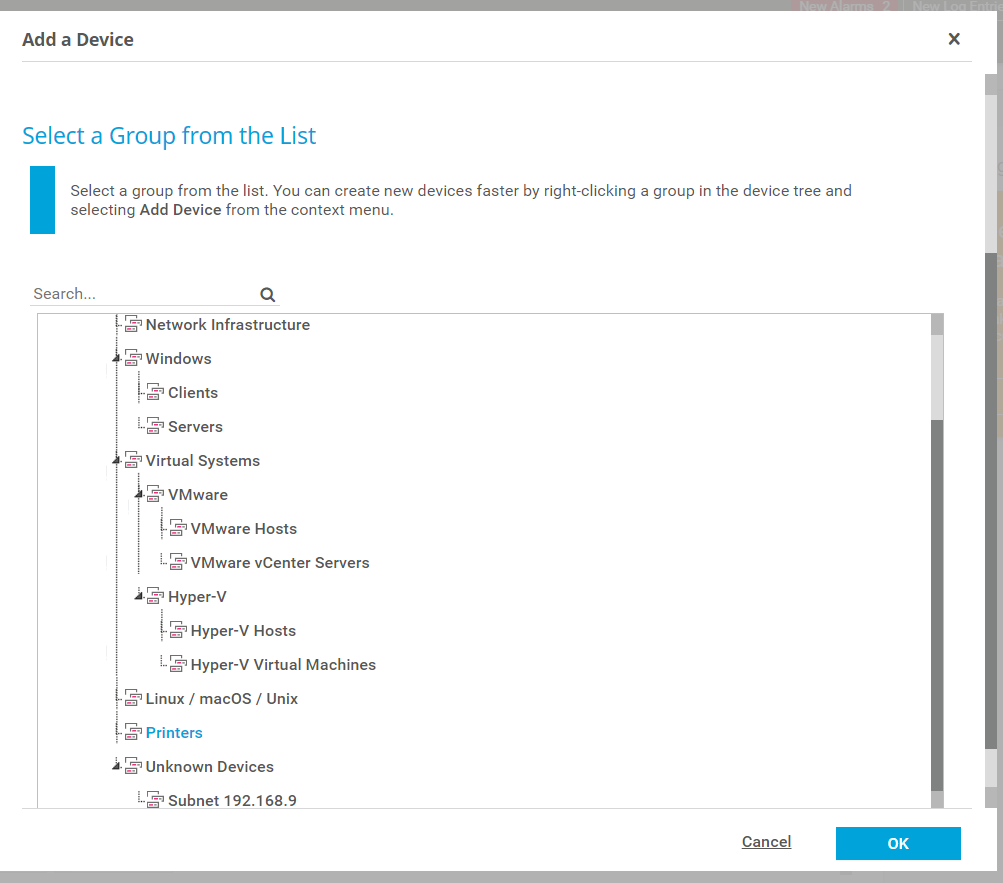
- Đăng nhập vào với quyền root

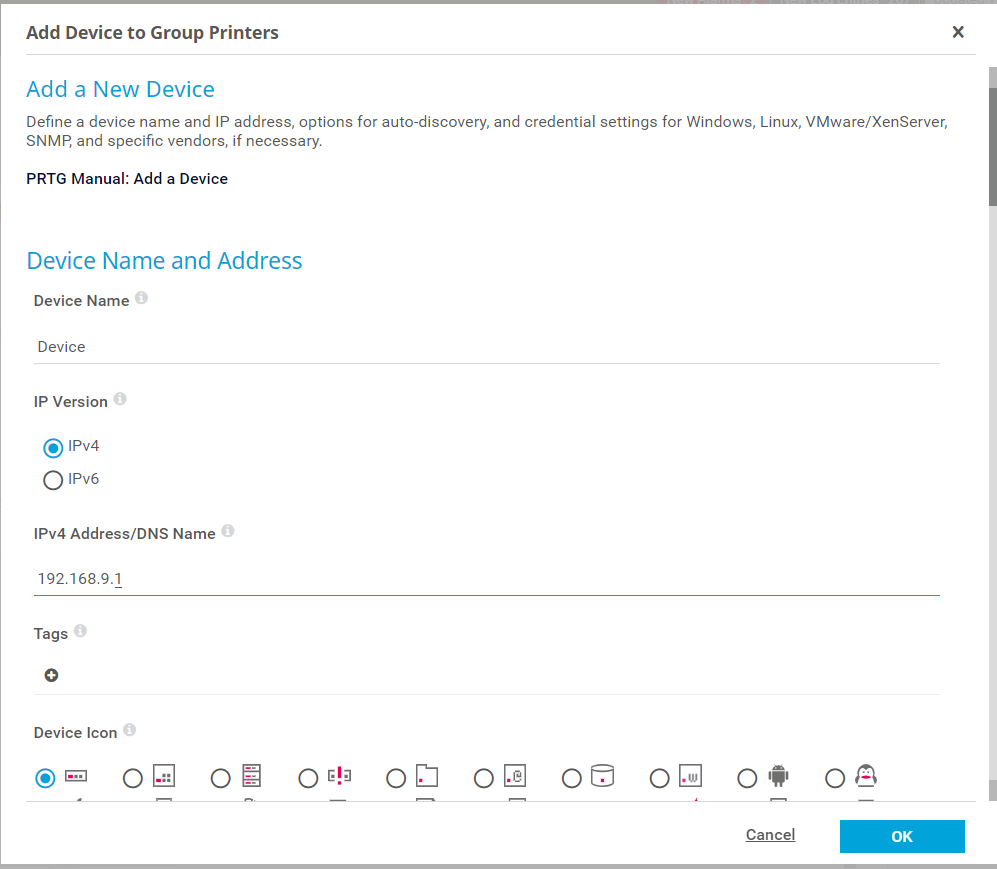


Thêm thiết bị để tiến hành giám sát

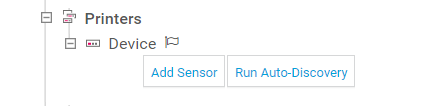


Lựa chọn thiết bị

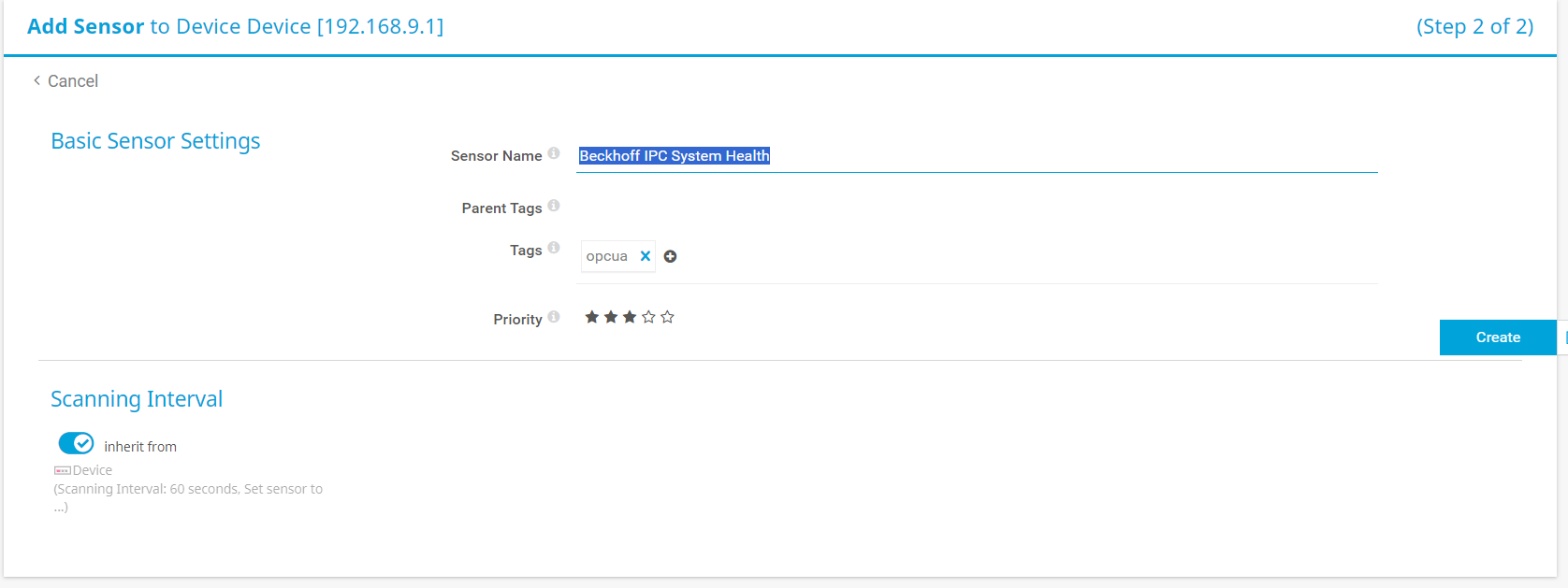




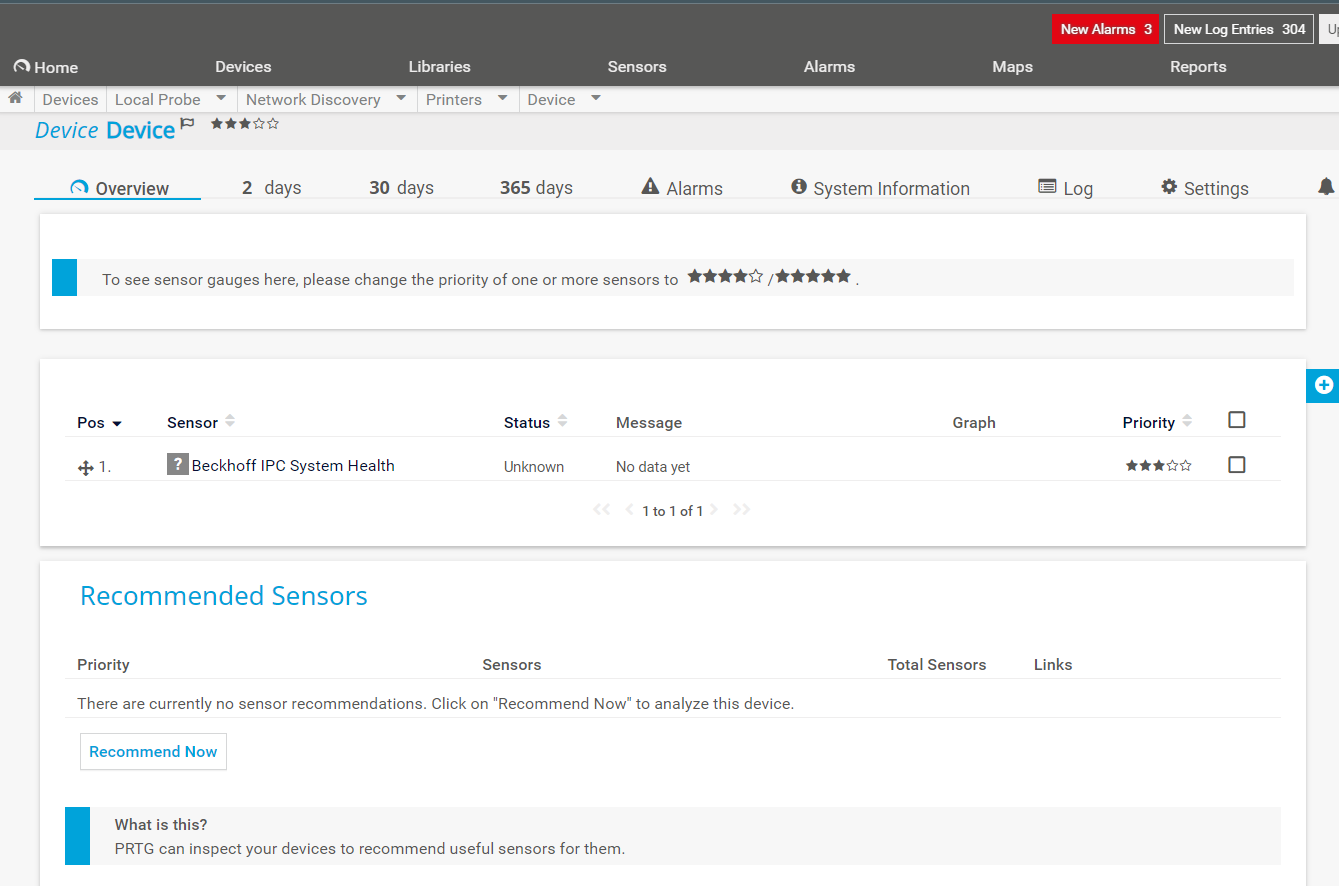
Chọn Add Sensor để thêm cảm biến



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



Add thành công



Ta 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.

