**SOC Analyst Project – Splunk SIEM Threat Detection & Alerting**

Phần I : Cài đặt và cấu hình

Bước 1: Chuẩn bị phần mềm và công cụ cần tải

| **Công cụ** | **Link / Ghi chú** |
| --- | --- |
| VMware Workstation / Player | VMware Workstation |
| VirtualBox | VirtualBox – dùng nếu muốn free |
| ISO Windows 11 | Tải từ trang chính Microsoft |
| ISO Ubuntu Server/Desktop | [Ubuntu](https://ubuntu.com/download/desktop?utm_source=chatgpt.com" \t "_new) |
| ISO Kali Linux | Kali |
| Splunk Free | Splunk Enterprise Free |
| Splunk Universal Forwarder | Splunk UF |
| Security Onion (Optional) | Security Onion |
| Tools khác | Sysmon (Windows), Wireshark (trên Kali), pfSense nếu muốn test firewall |

Bước 2: Tạo mạng LAN ảo

Trong VMWare Workstation Pro

Mở VMware → Edit > Virtual Network Editor

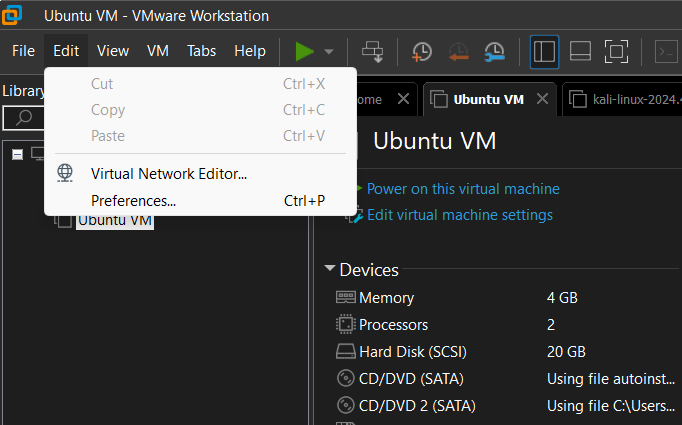
Click Add Network, chọn VMnet2 (ví dụ) → OK

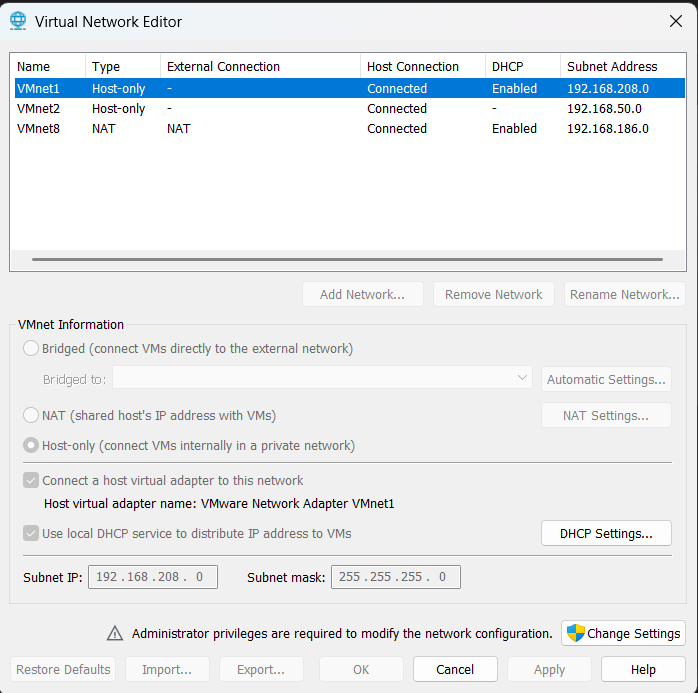
Chọn kiểu Host-Only → chỉ cho VM giao tiếp với nhau, không ra Internet

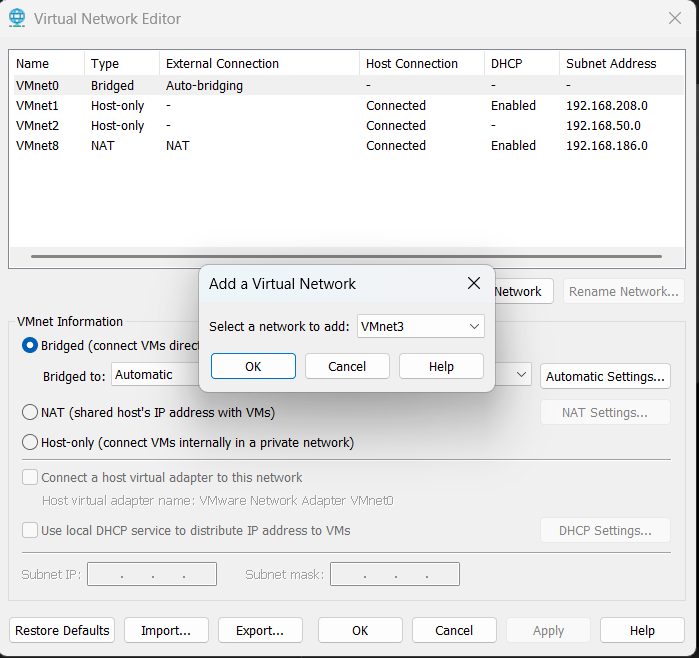
Cấu hình:

* Subnet IP: 192.168.50.0
* Subnet mask: 255.255.255.0
* DHCP: tắt (dùng IP tĩnh để dễ viết detection rule)

Nhấn Apply → OK









Bước 3: Tạo và cấu hình VM

Windows 11 (Client / Test PowerShell)

Cấu hình VM:

ISO Windows 11

RAM ≥ 4GB

CPU ≥ 2 core

HDD ≥ 60GB

Network:

Edit VM → Network Adapter → Custom: VMnet2

IP tĩnh:

IP: 192.168.50.10

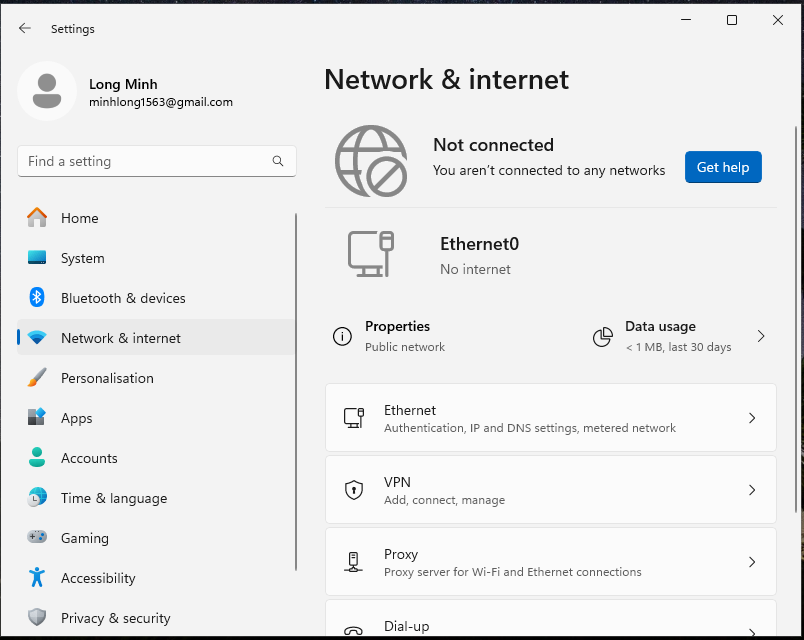
Subnet: 255.255.255.0

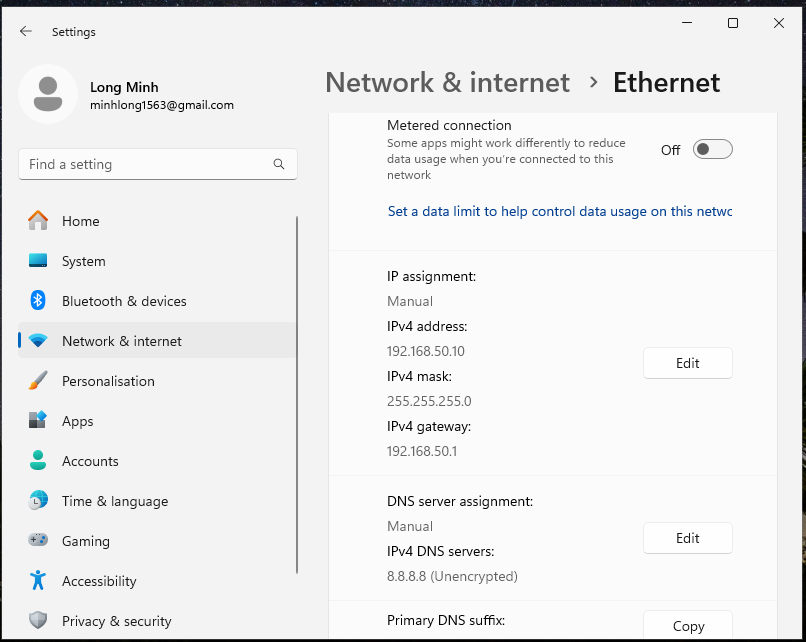
Gateway: 192.168.50.1

Cài log collection:

Install Splunk Universal Forwarder → forward logs tới Splunk Server 192.168.50.40

Install Sysmon → log các sự kiện Process Create, Network Connect, PowerShell





Ubuntu (Linux Server / Syslog)

Cấu hình VM:

RAM ≥ 2GB

CPU ≥ 1 core

HDD ≥ 20GB

IP tĩnh: 192.168.50.20

Cài log forwarder:

sudo apt update && sudo apt install rsyslog

sudo nano /etc/rsyslog.d/50-default.conf

# Thêm dòng cuối file:

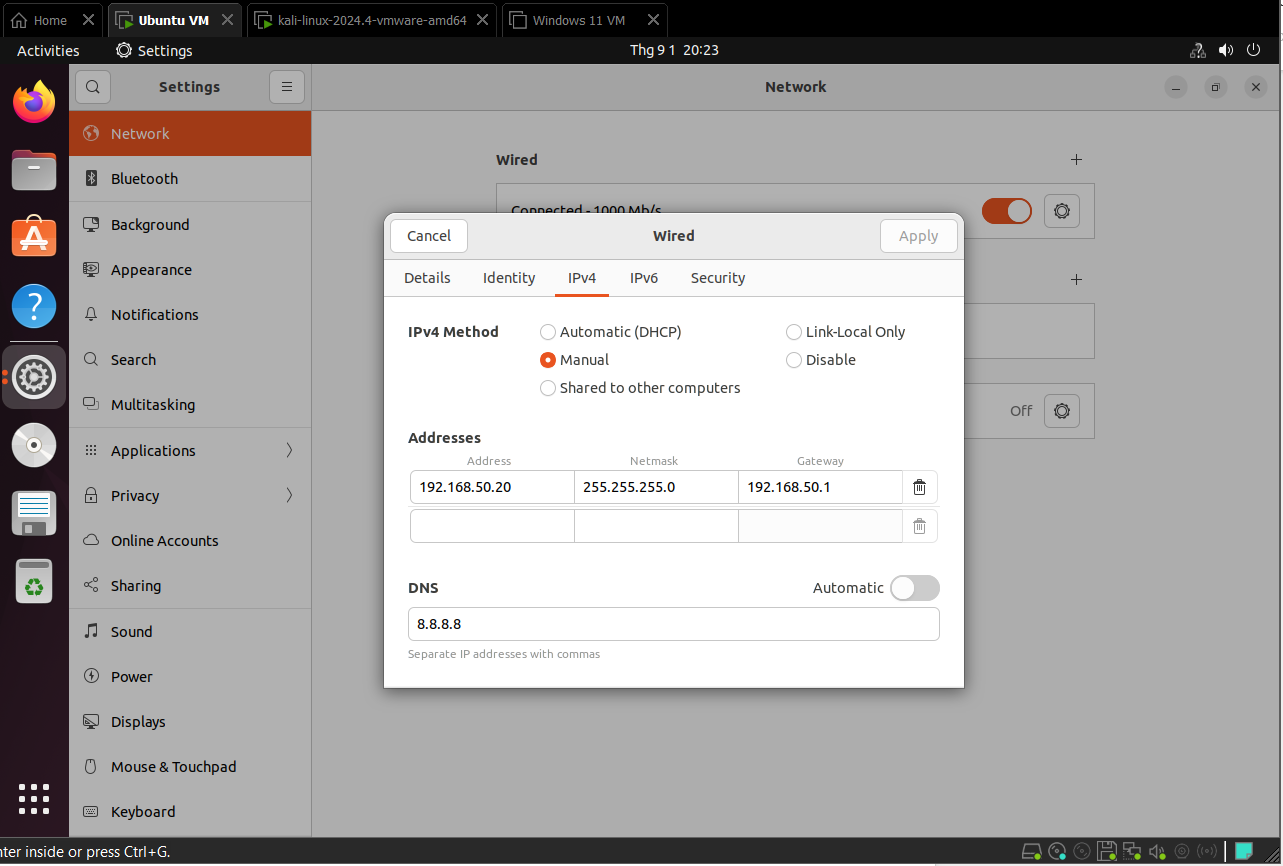
\*.\* @@192.168.50.40:514

sudo systemctl restart rsyslog

Collect logs:

/var/log/auth.log → login attempts

/var/log/syslog → system events



Kali Linux (Attacker VM)

Cấu hình VM:

RAM ≥ 2GB

CPU ≥ 1 core

HDD ≥ 20GB

IP tĩnh: 192.168.50.30

Tools: hydra, nmap, curl, Wireshark

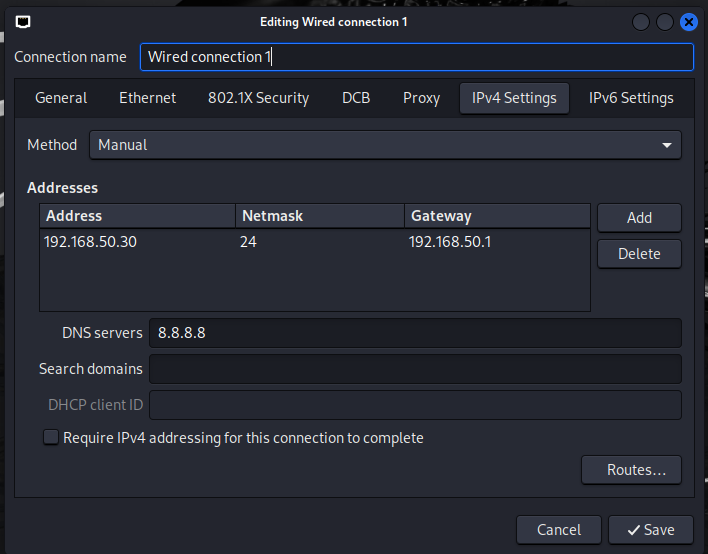
Mục đích: simulate attack:

SSH brute-force Windows/Ubuntu

Phishing test (safely)

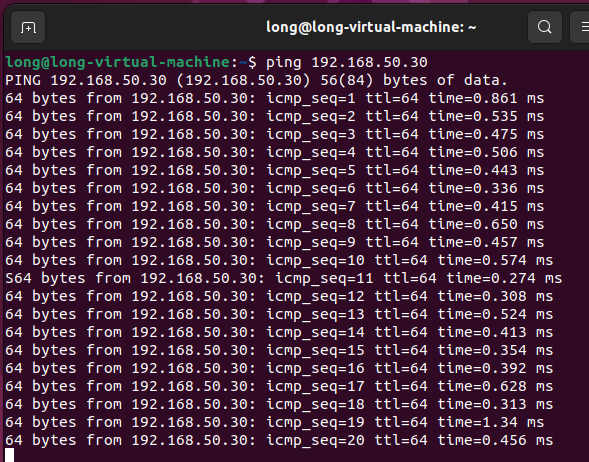
File copy / exfiltration



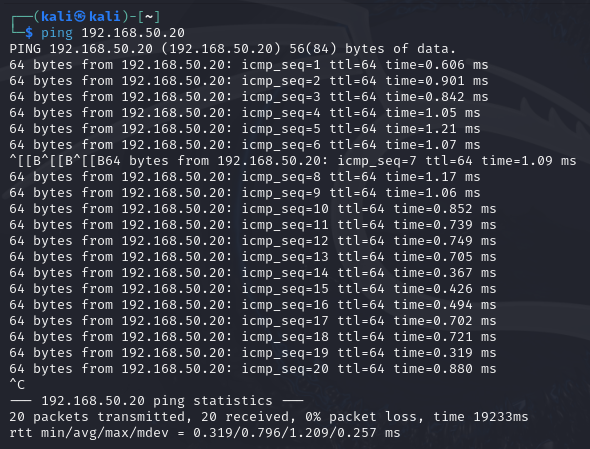


Bước 4: kiểm tra kết nối mạng giữa các máy

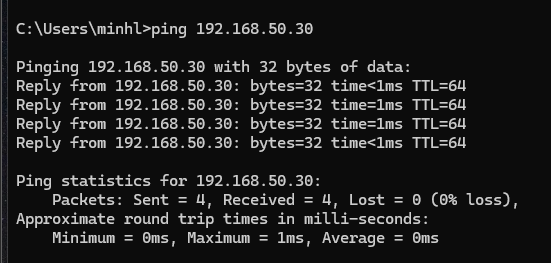
Ping giữa các VM  
Ping từ Ubuntu sang Kali linux



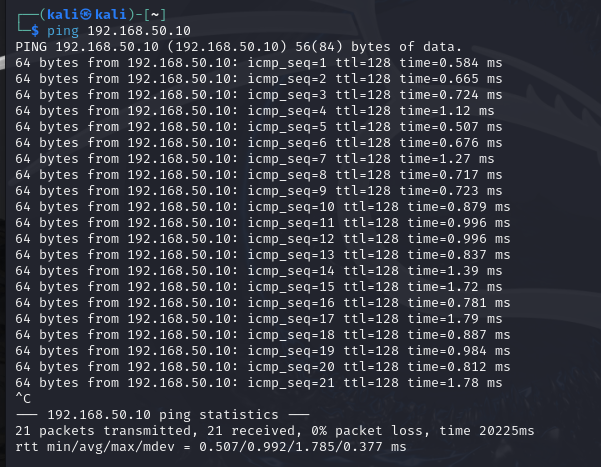
Ping từ Kali linux sang Ubuntu



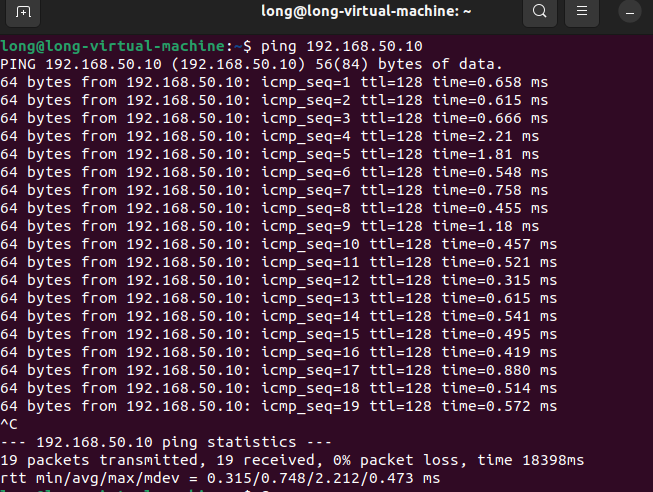
Ping từ Windows11 sang Kali Linux



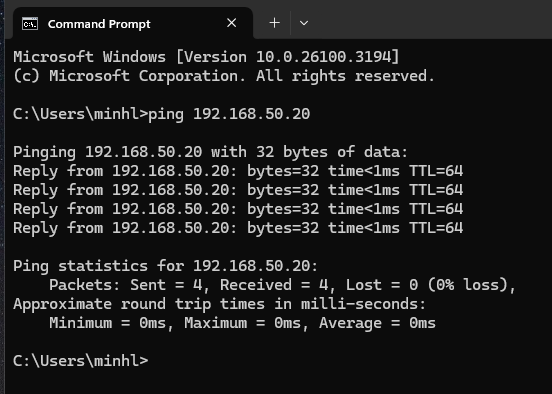
Ping từ Kali Linux sang Windows11



Ping từ Ubuntu sang Windows11



Ping từ Windows11 sang Ubuntu

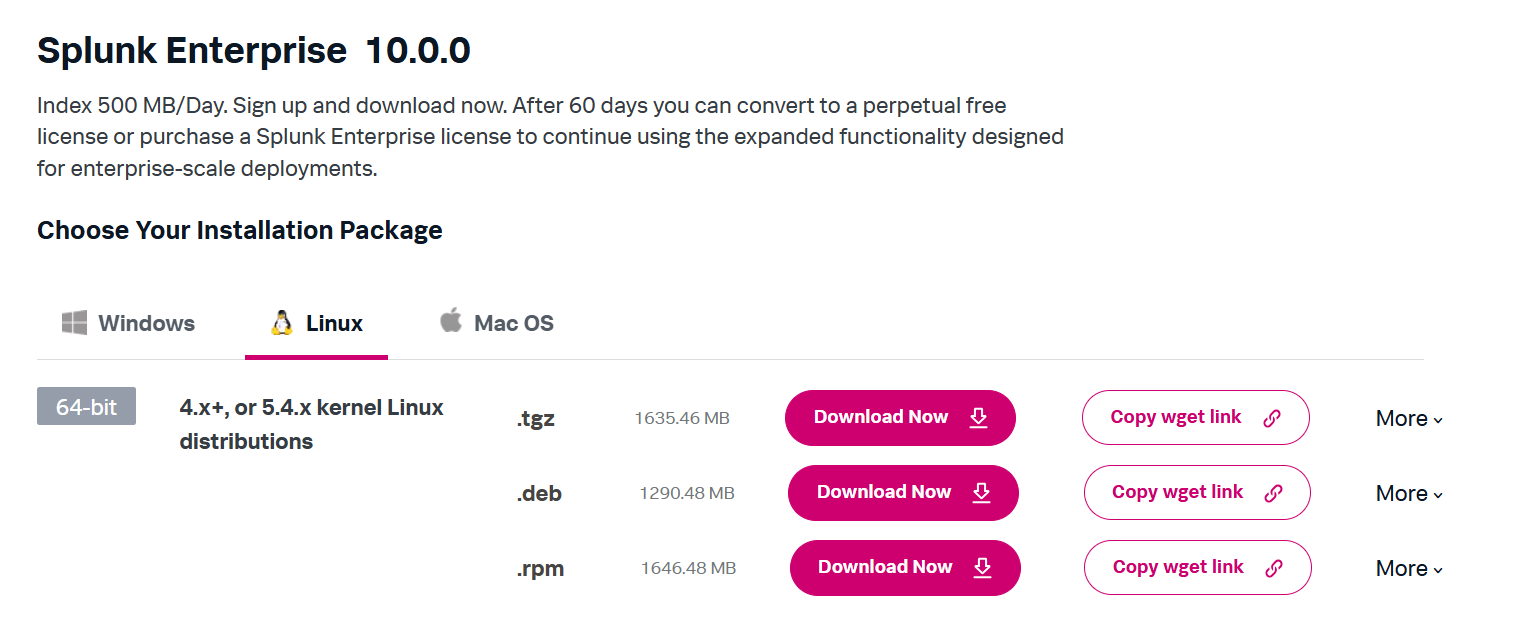


=> Kết nối giữa các máy trên Mạng LAN ảo VMNET2 thành công.

Bước 5:

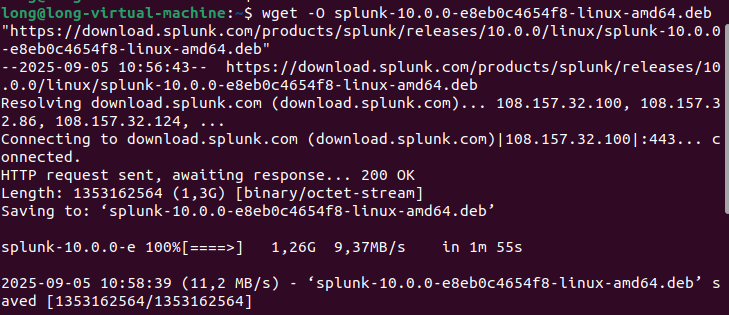
Cài Splunk Enterprise cho Ubuntu 192.168.50.20 (SIEM Server)

Truy cập và tạo tài khoản splunk Enterprise:

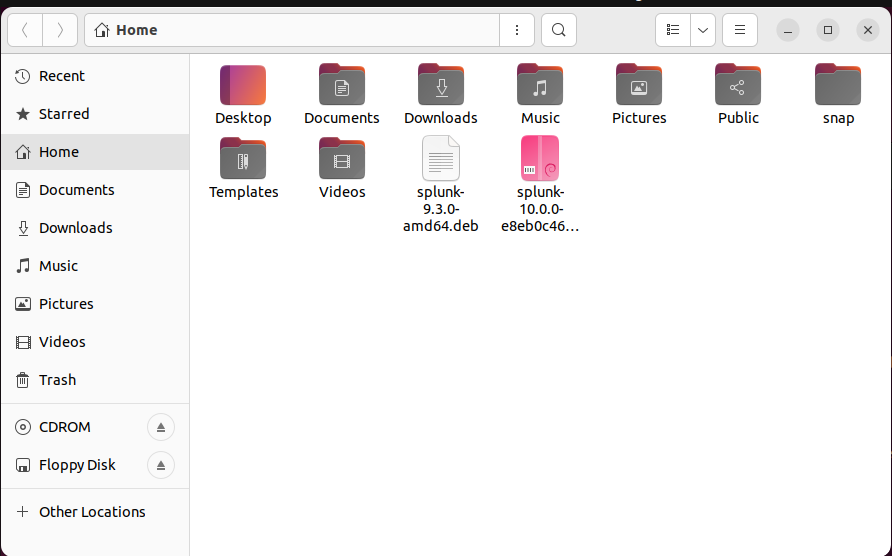


Copy wget link .deb dành cho Linux, copy rồi dán chạy lệnh

wget -O splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb "https://download.splunk.com/products/splunk/releases/10.0.0/linux/splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb"

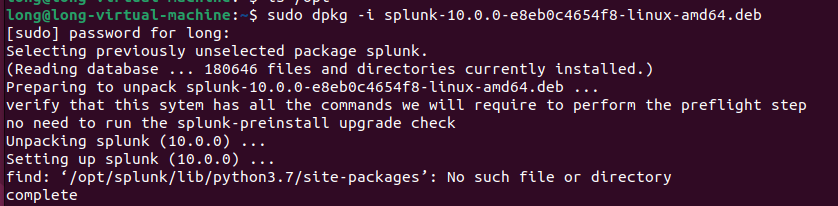


Sau khi cài thành công Splunk thì dùng lệnh để unpack gói cài



Ở đây ta dung lệnh:

sudo dpkg -i splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb

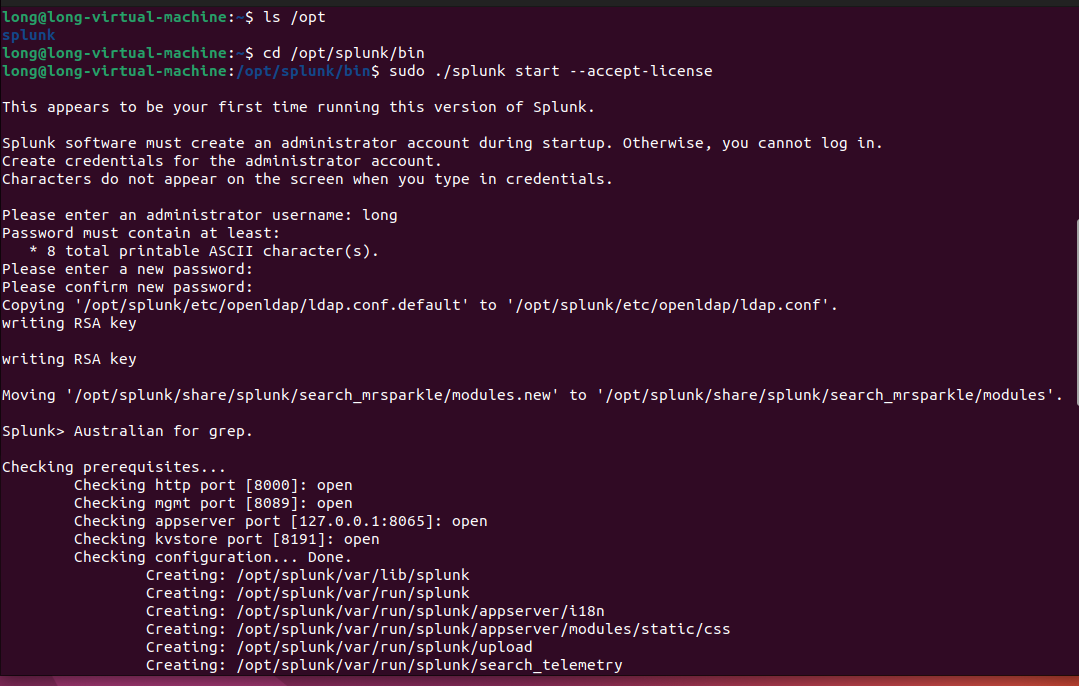


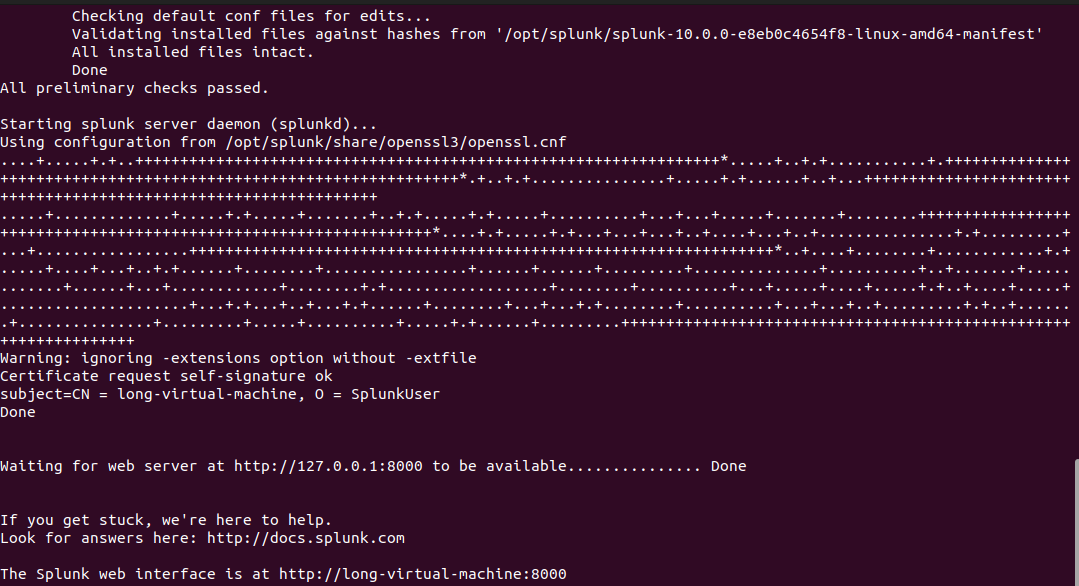
Sau đó ta kiểm tra tệp trong /opt bằng lệnh ls /opt

Sau đó cd vào /opt/splunk/bin

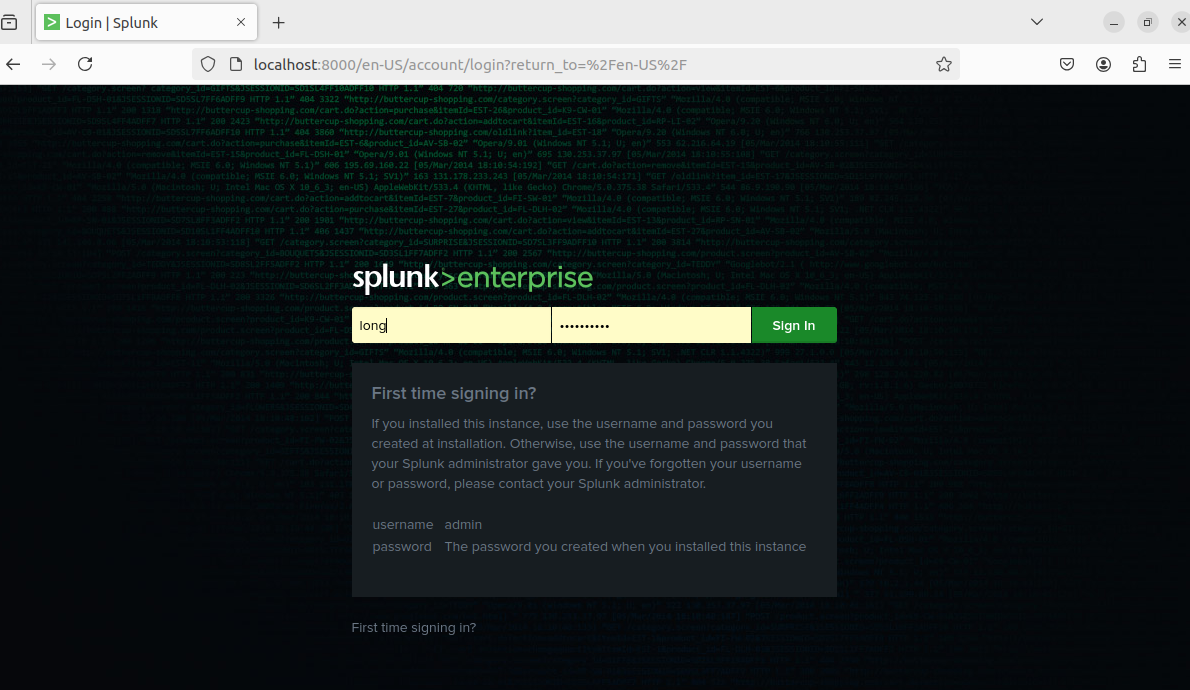
Khi đã vào tệp ta chạy lệnh sudo ./splunk start --accept-license để khởi dộng splunk

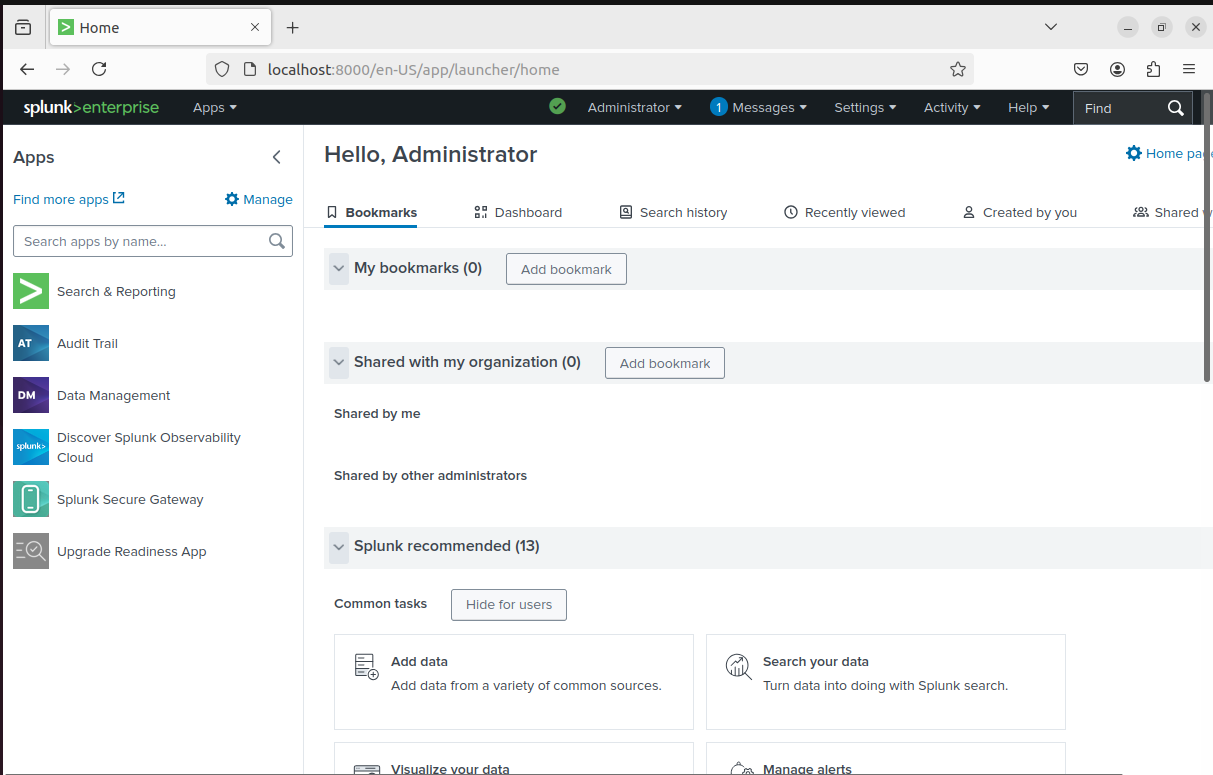
Trước khi khởi động splunk yêu cầu tạo username và password



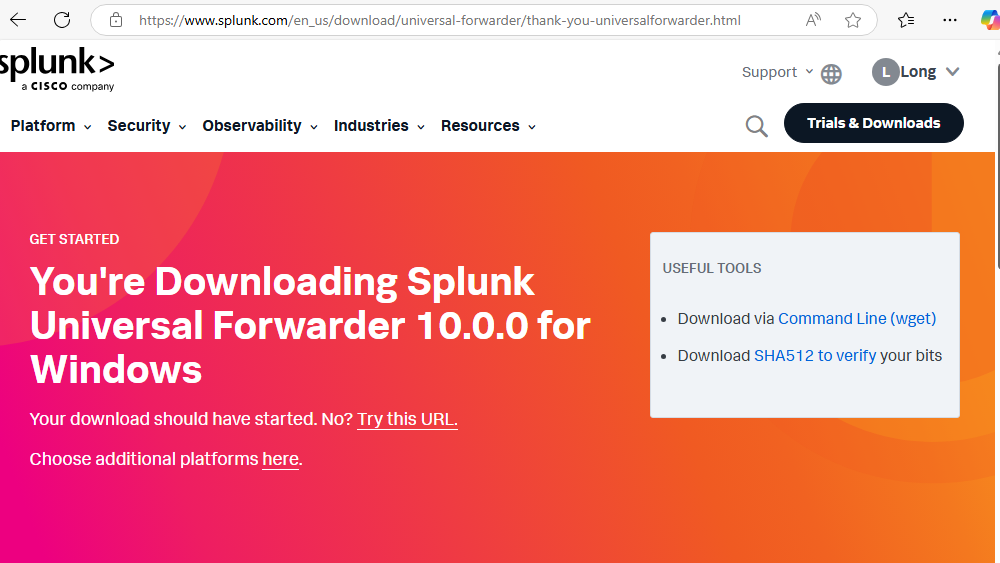


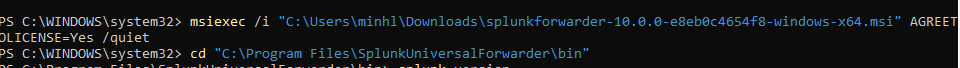
Sau khi khởi động ta có web interface với địa chỉ: <http://long-virtual-machine:8000>





Cài Splunk Universal Forwarder trên Windows11 VM







Cài đặt thành công Splunk Universal Forwarder trên Windows11 VM

Kết nối Splunk Enterprise với Splunk Universal Forwarder: