

LAB 03 – NETWORK MONITOR&ANALYSIS

Môi trường thực hành:

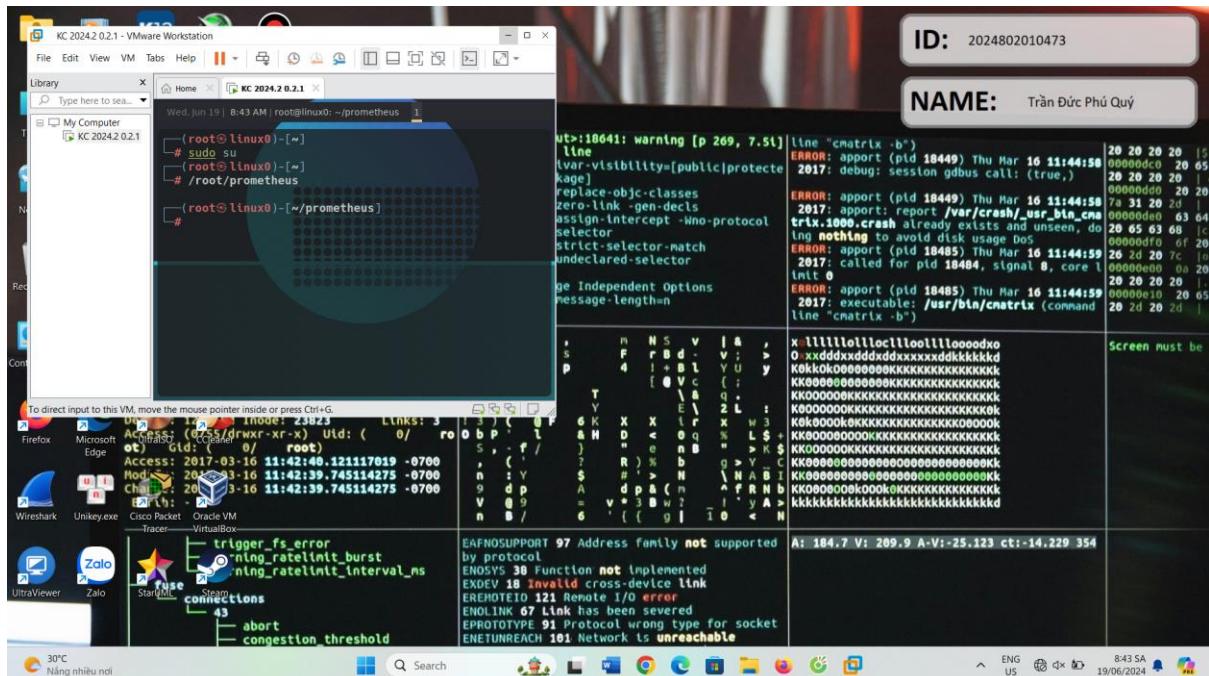
2 Máy ảo (VM): Monitor, Server

Các công cụ: Prometheus, Grafana, Nessus

1. PROMETHEUS (4D)

Trên Monitor, Đăng nhập với quyền root

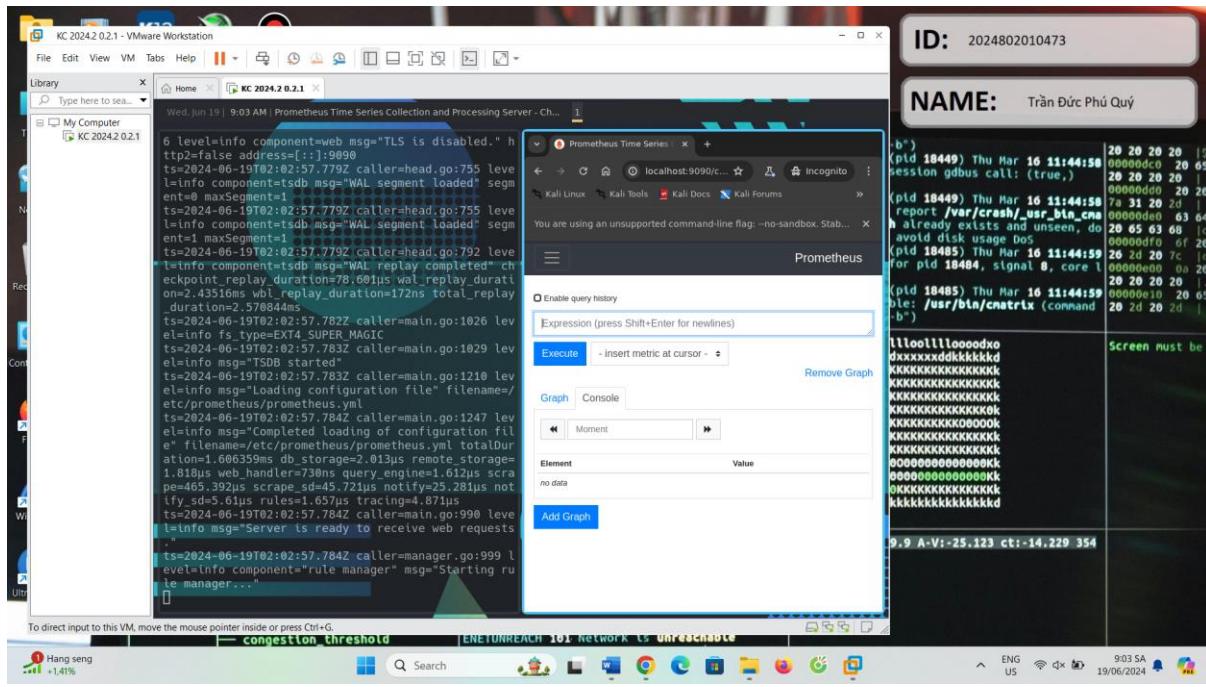
1.1. Di chuyển vào thư mục ~ /prometheus, thực hiện lệnh kiểm tra phiên bản



Gợi ý: tham số --version

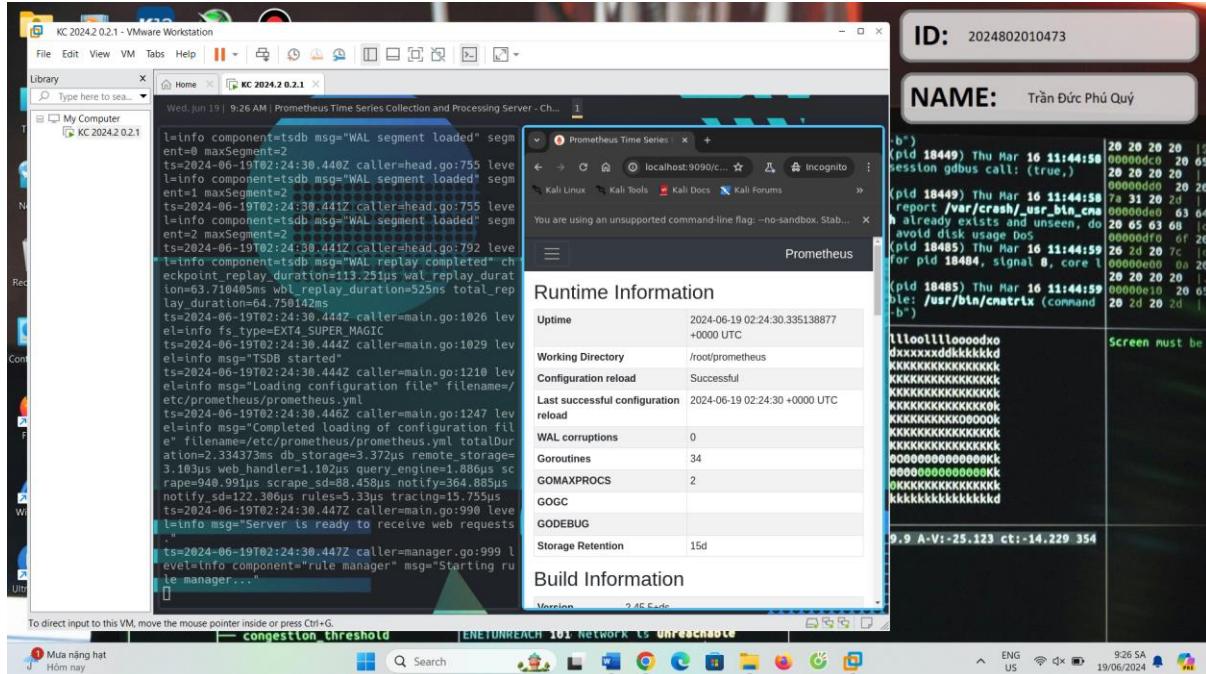
1.2. Thực hiện lệnh khởi chạy prometheus

1.3. Mở giao diện web chính prometheus



Gợi ý: Chromium = Windows + W , port 9090

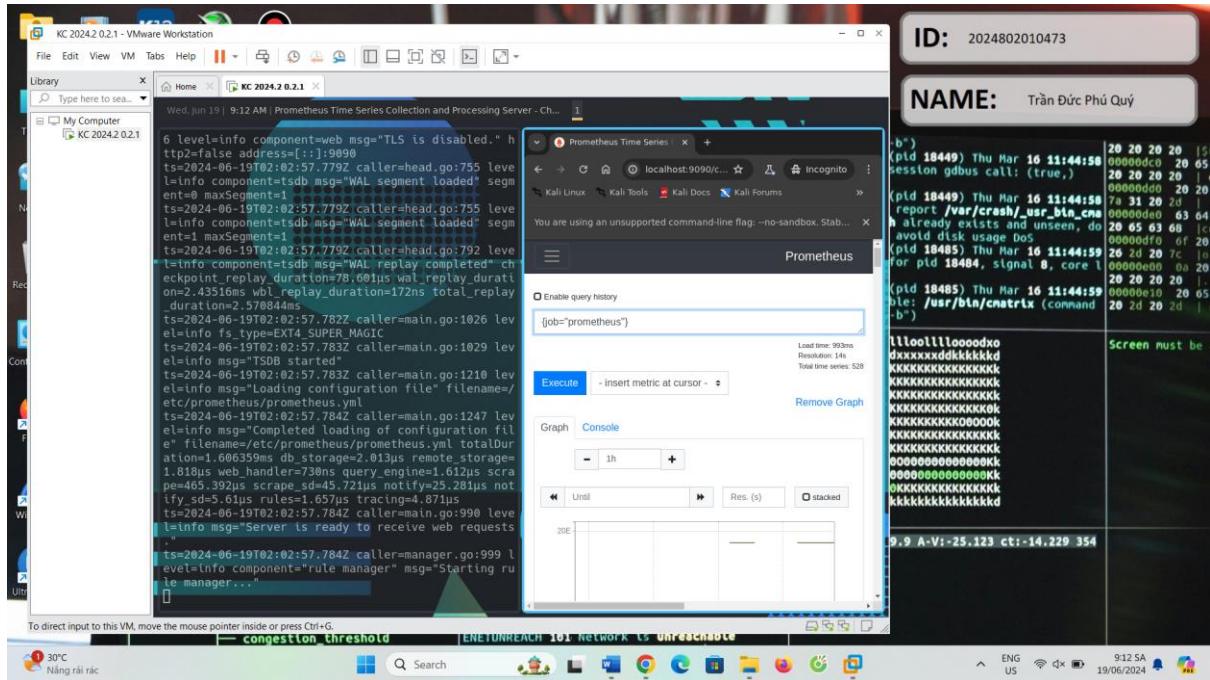
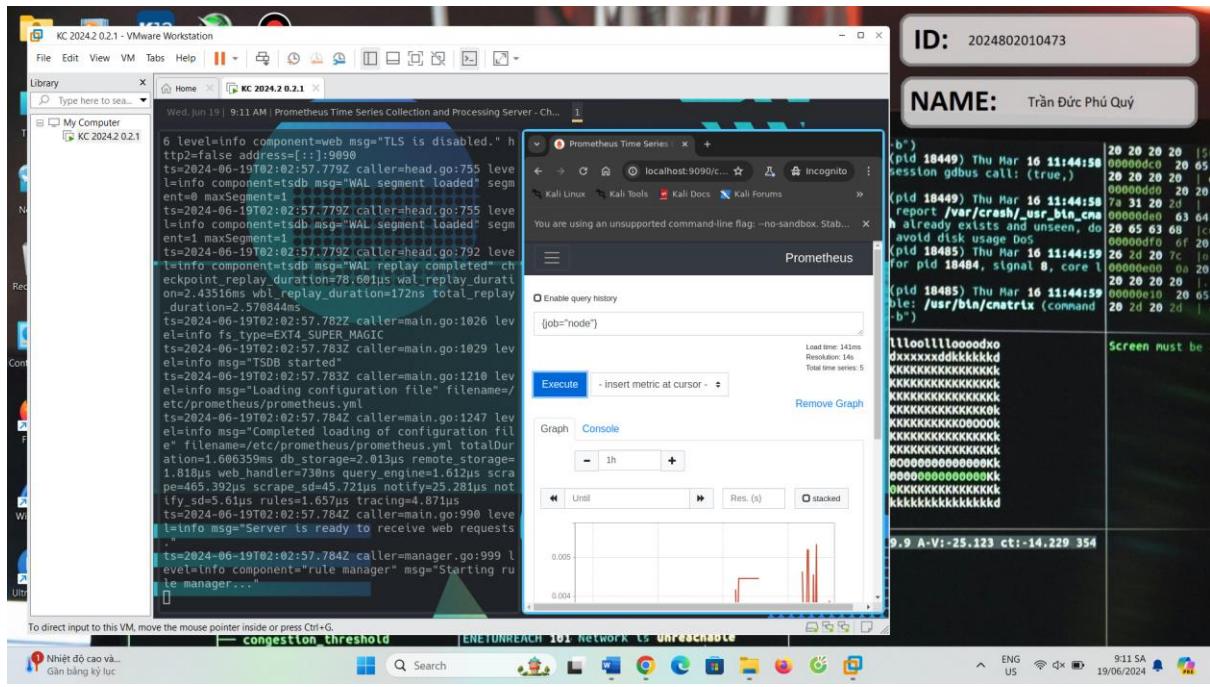
1.3. Mở giao diện kiểm tra job đang chạy:

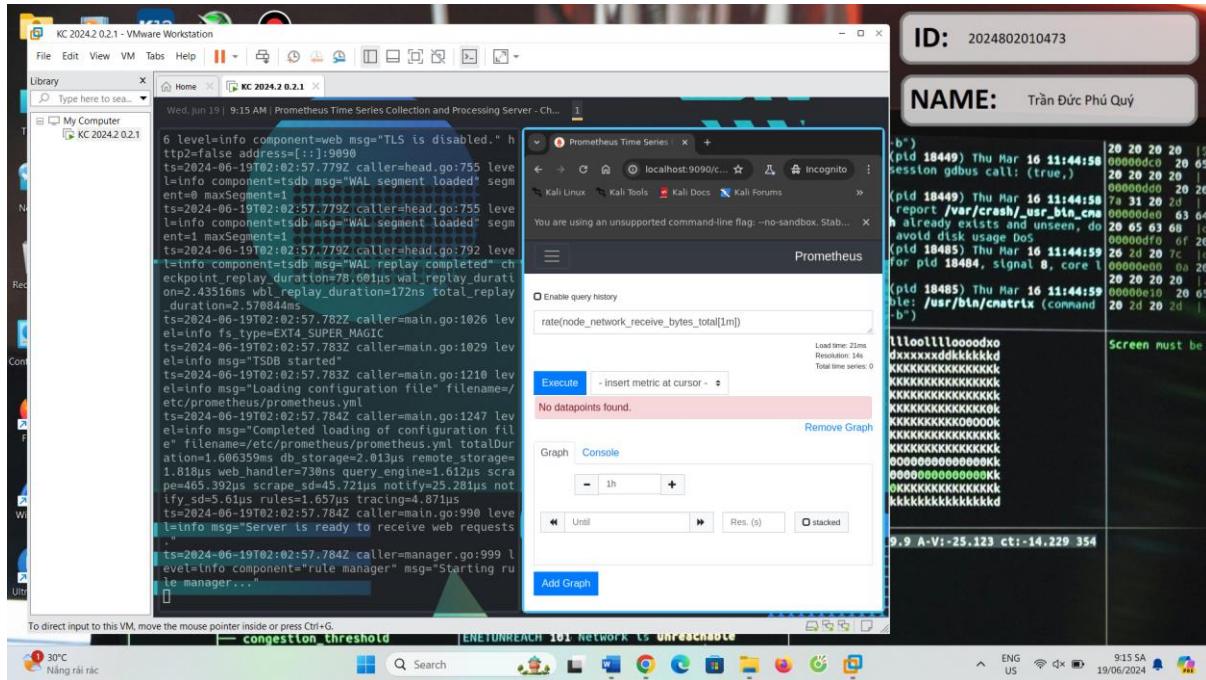
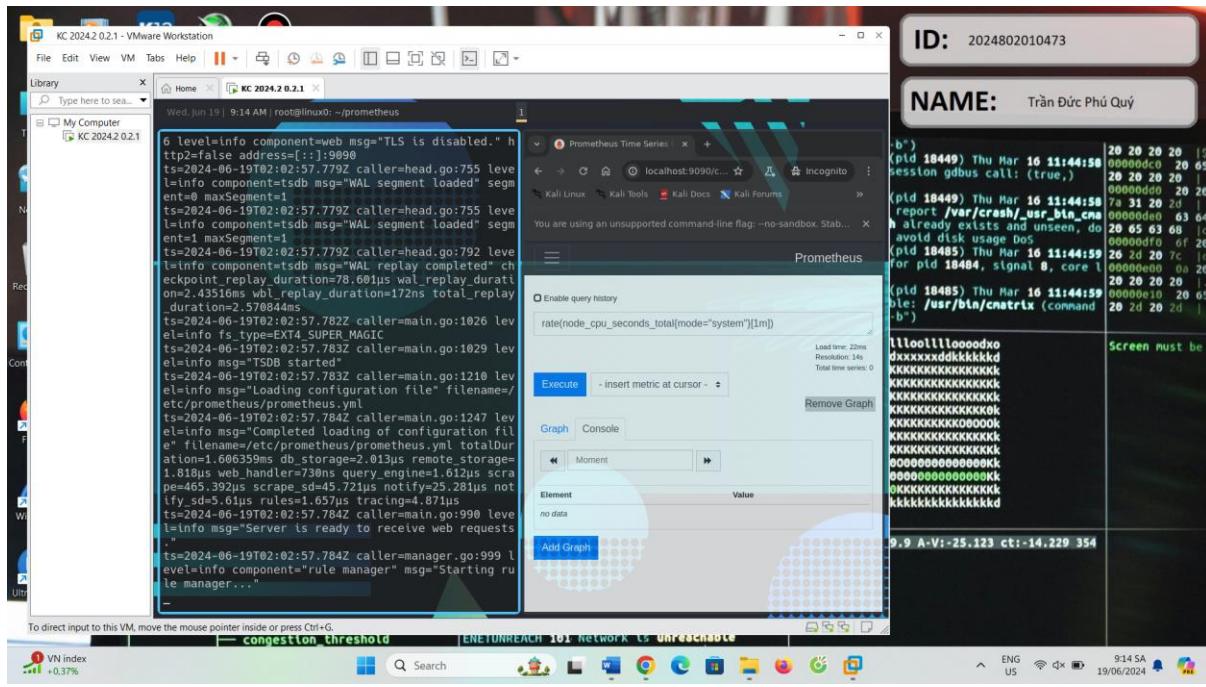


Gợi ý: <http://<url>/tsdb-status>

1.4. Mở giao diện truy vấn dữ liệu, thử truy vấn dữ liệu sau

```
{job="node"}
{job="prometheus"}[5m]
rate(node_cpu_seconds_total{mode="system"})[1m]
rate(node_network_receive_bytes_total[1m])
```





Gợi ý: <http://<url>/graph>

1.5. Ngưng ứng dụng prometheus, cấu hình lại tập tin prometheus.

my global config

global:

```
scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is
every 1 minute.

evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every
1 minute.

# scrape_timeout is set to the global default (10s).

# Alertmanager configuration

alerting:
  alertmanagers:
    - static_configs:
        - targets:
          # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global
'evaluation_interval'.

rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:

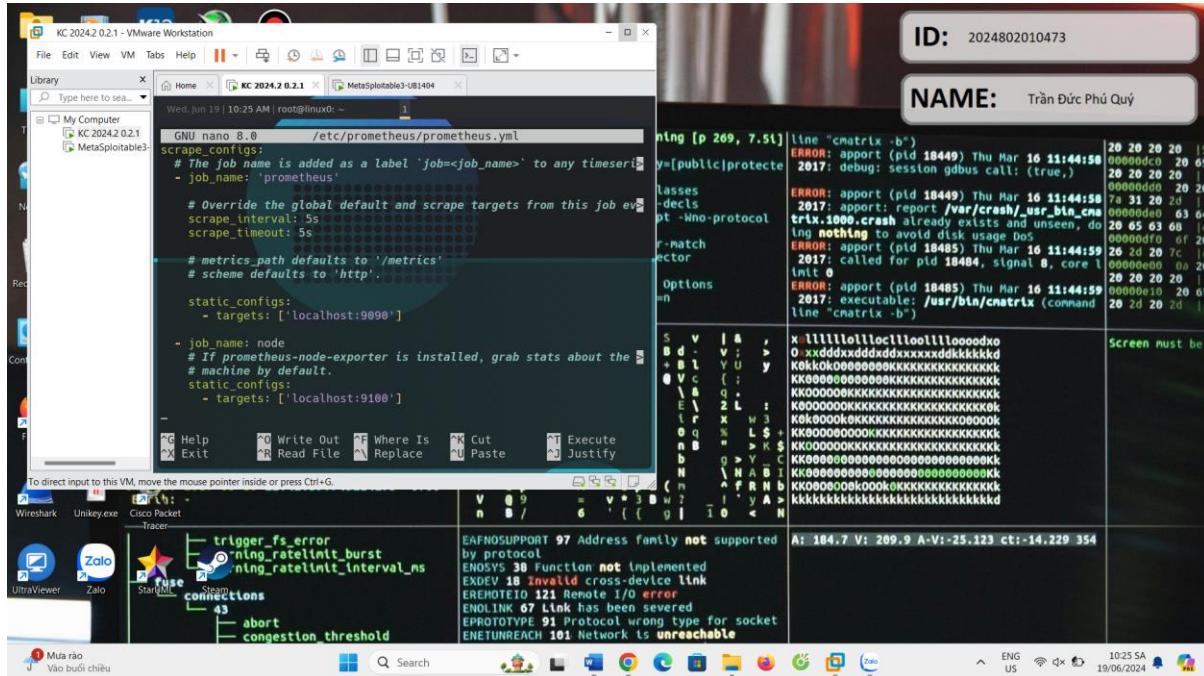
# Here it's Prometheus itself.

scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped
  # from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

static_configs:
```

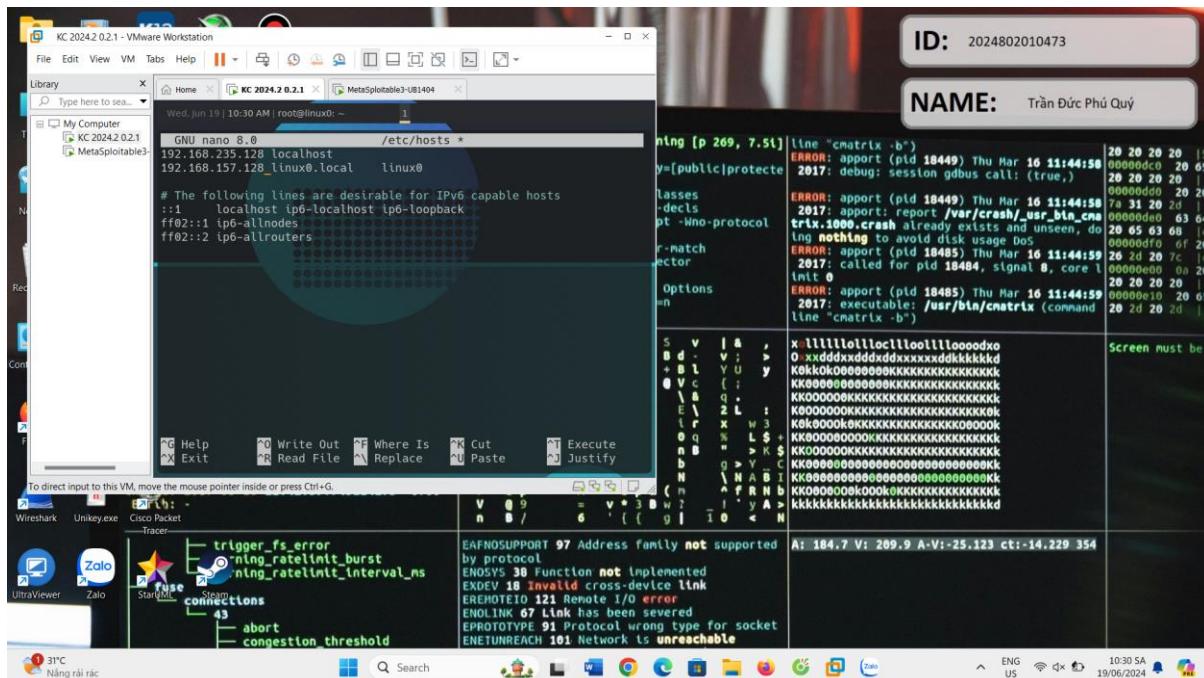
- targets: ["localhost:9090"]



1.6. sửa tệp "/etc/hosts" thêm vào các dòng sau vào cuối tệp:

x.x.x.x monitor

y.y.y.y server



Gợi ý: x.x.x.x là IP Monitor , y.y.y.y là IP Server

1.7. Để thu thập dữ liệu từ **Monitor** và **Server** chúng ta thêm job mới tên là “node”, cụ thể xem phần dưới.

```
# my global config

global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is
  # every 1 minute.

  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every
  # 1 minute.

  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration

alerting:
  alertmanagers:
    - static_configs:
        - targets:
            # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global
# 'evaluation_interval'.

rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:

# Here it's Prometheus itself.

scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped
  # from this config.

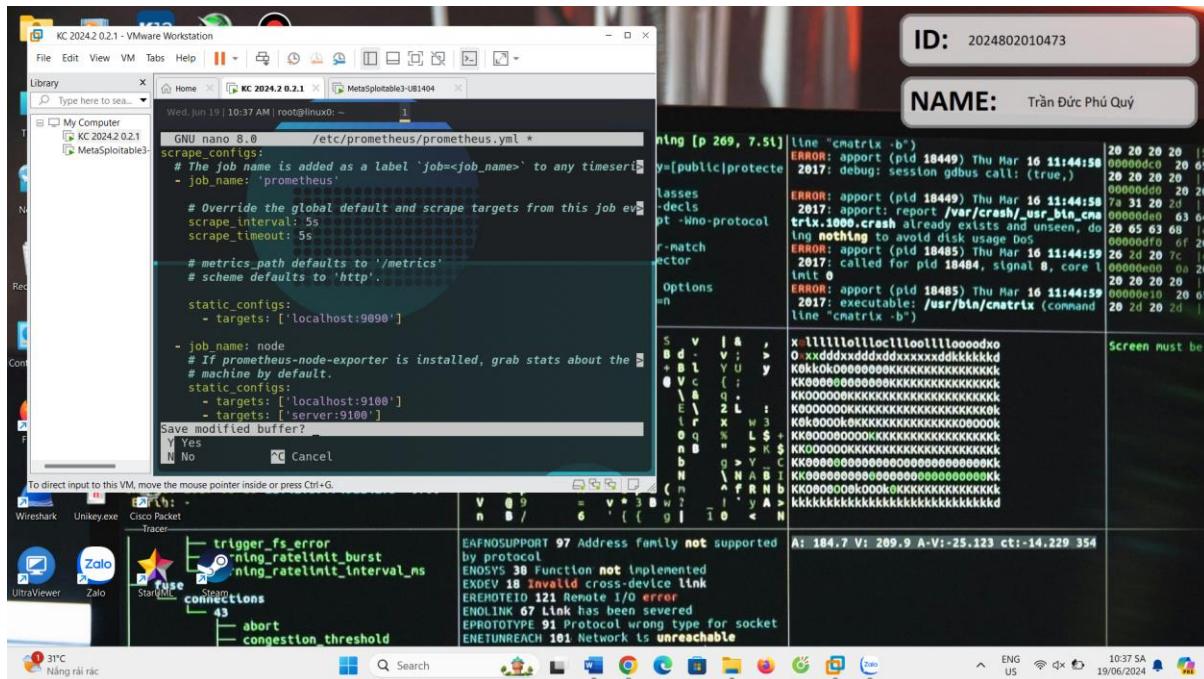
  - job_name: "prometheus"

    static_configs:
```

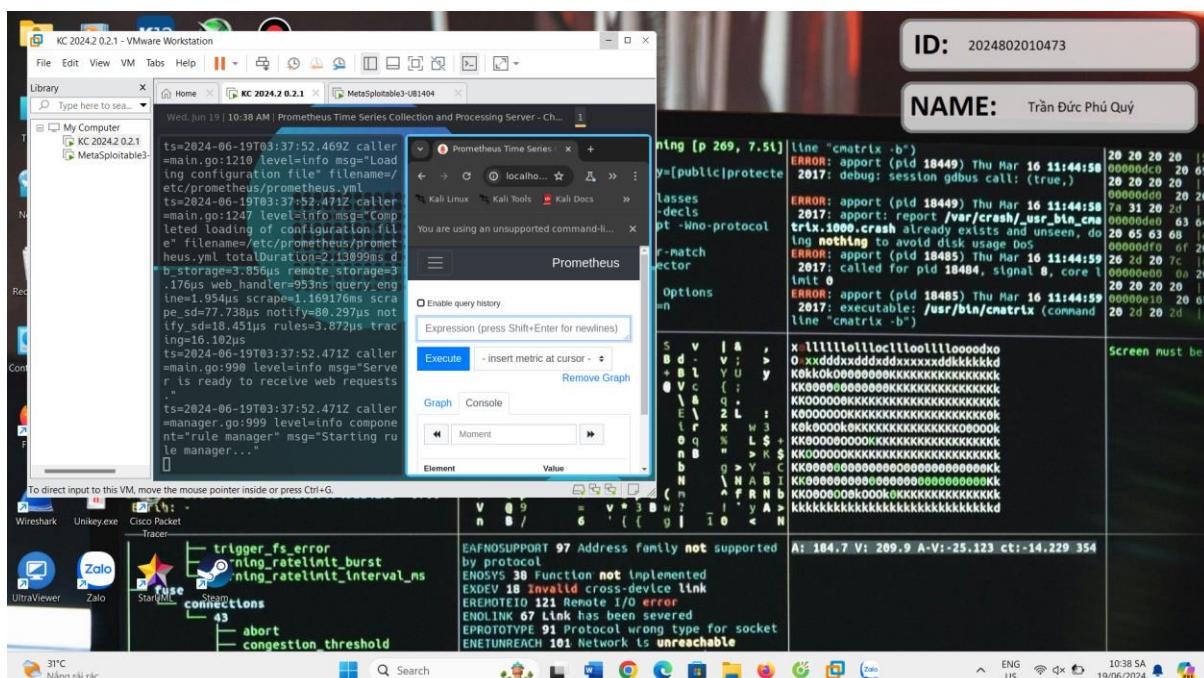
- targets: ["localhost:9090"]
- job_name: "node"

static_configs:

- targets: ["monitor:9100"]
- targets: ["server:9100"]



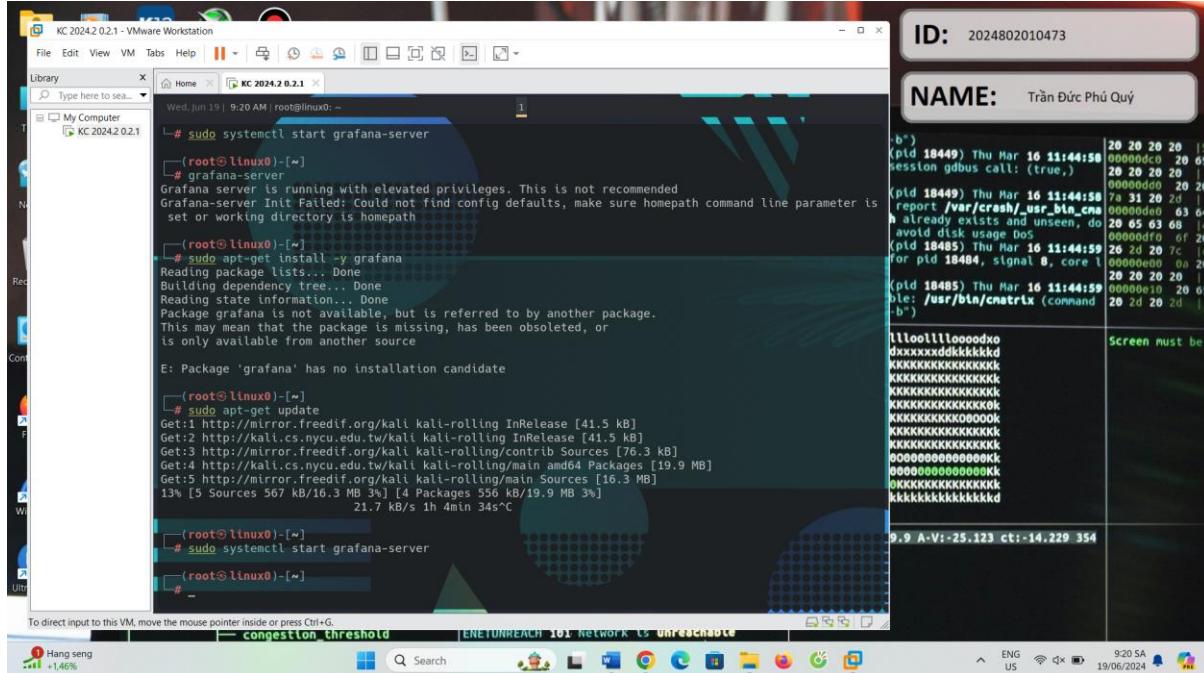
1.8. Chạy lại prometheus theo cấu hình này.



2. GRAFANA (3D)

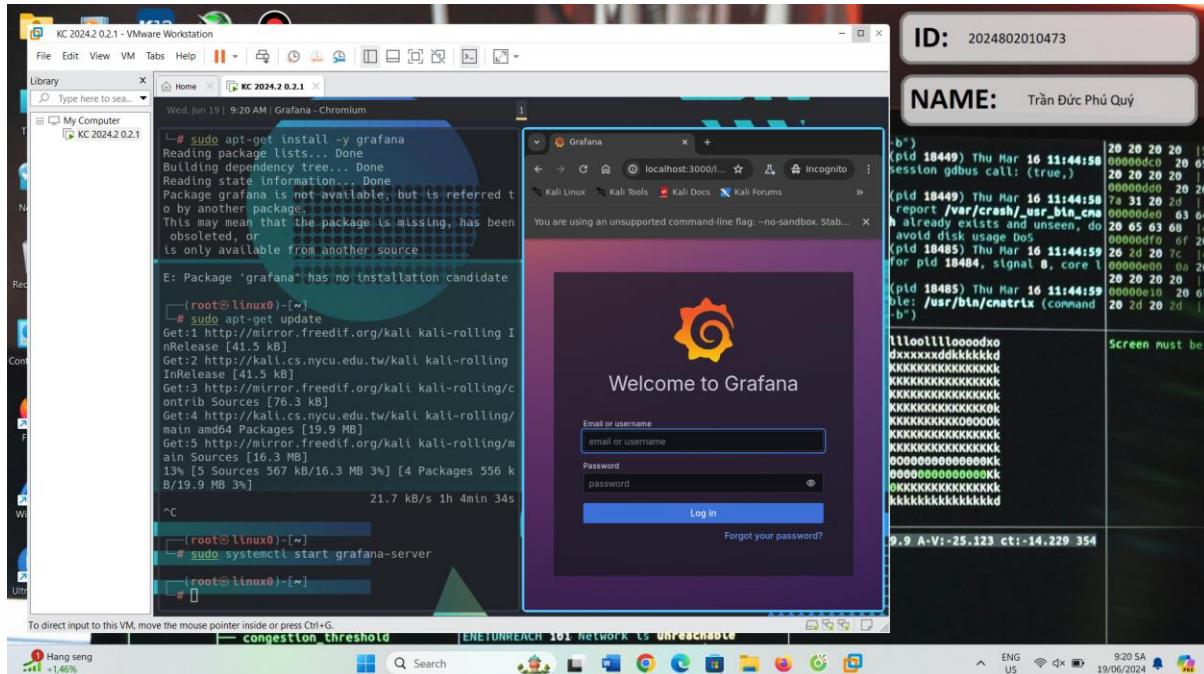
Trên Monitor, Đăng nhập với quyền root

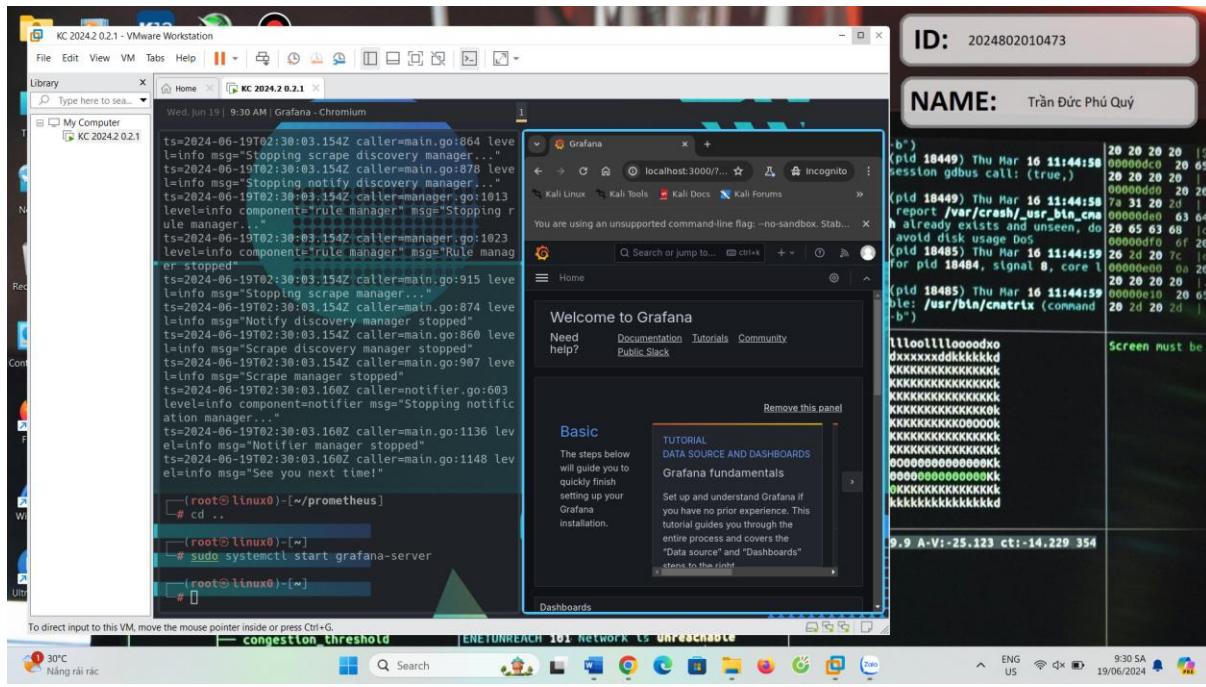
2.1. Dùng lệnh khởi chạy dịch vụ Grafana



Gợi ý: grafana-server

2.2. Mở giao diện web của grafana





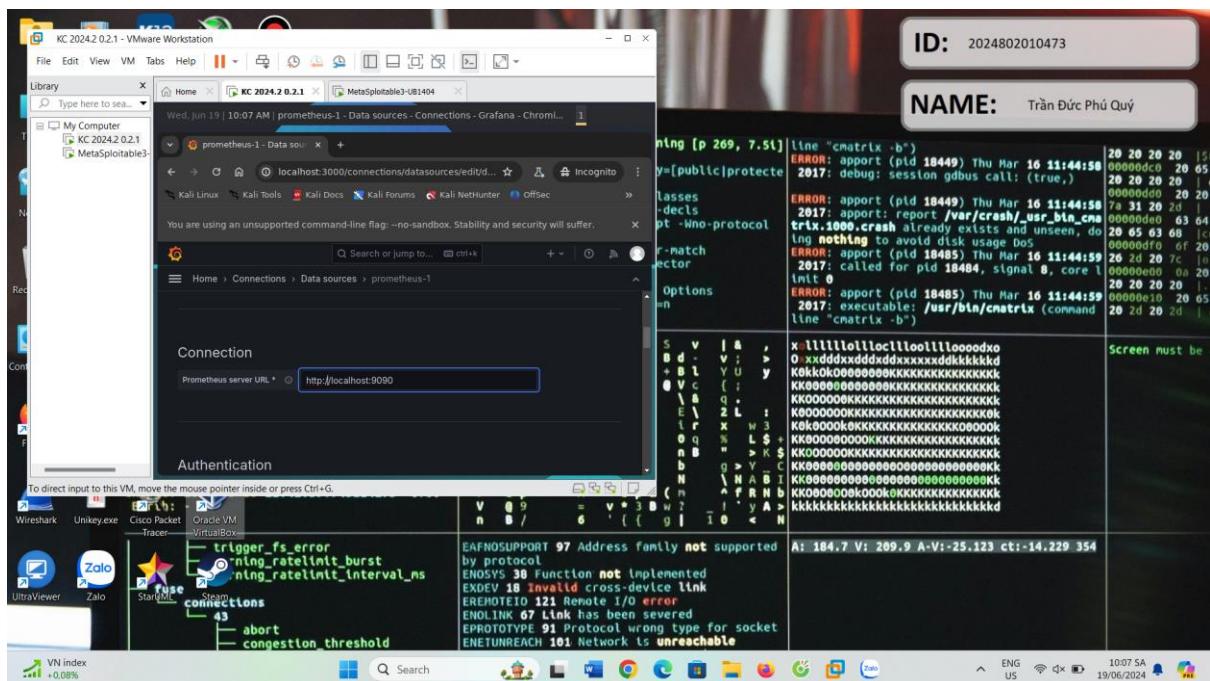
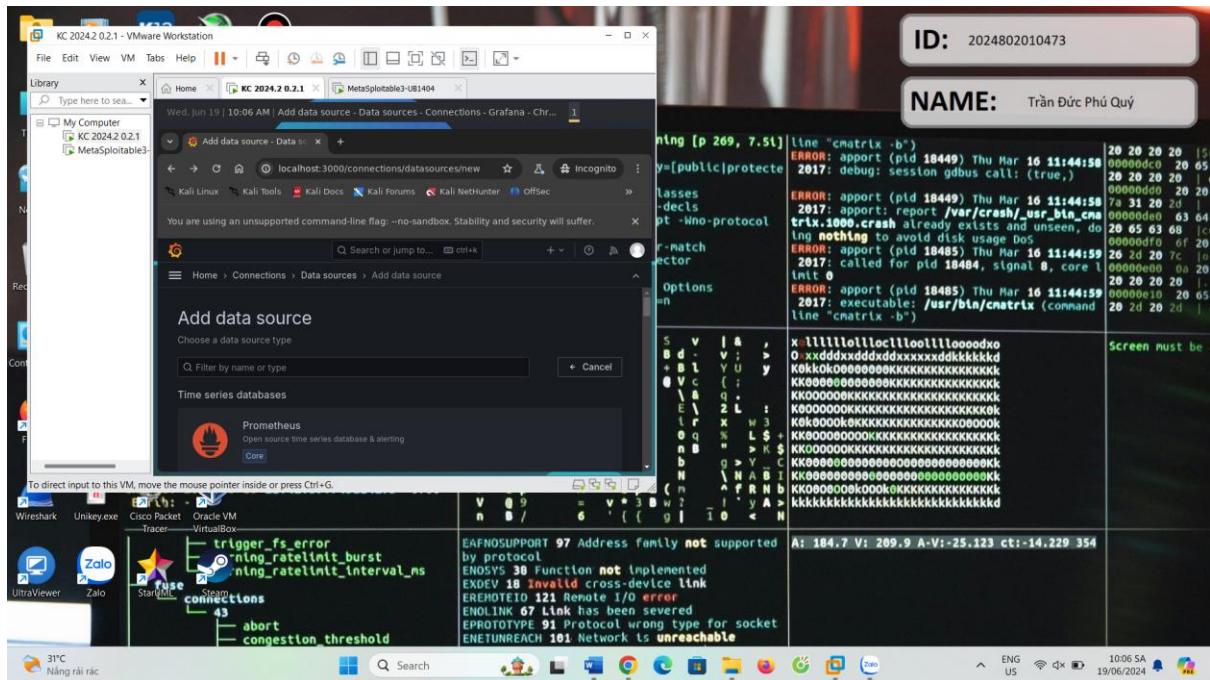
Gợi ý: Chromium = Windows + W , port 3000

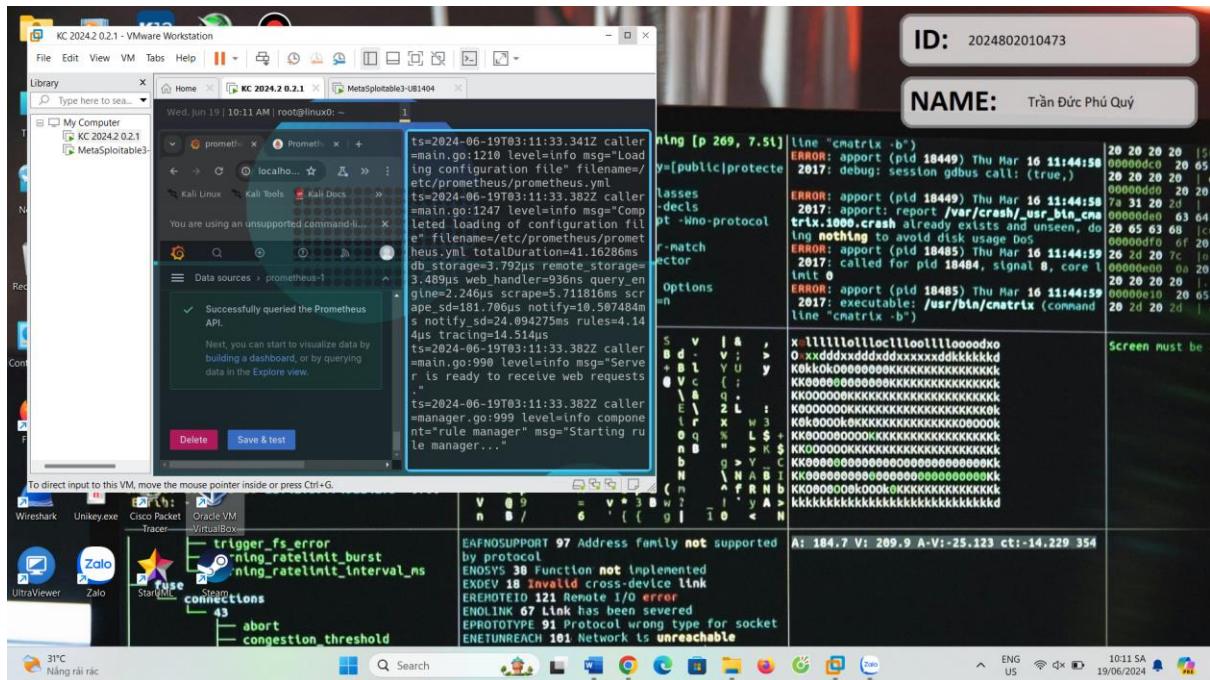
2.2. Cấu hình hiển thị grafana

Làm 2 bước sau

1. Thêm mới “Data Source”:

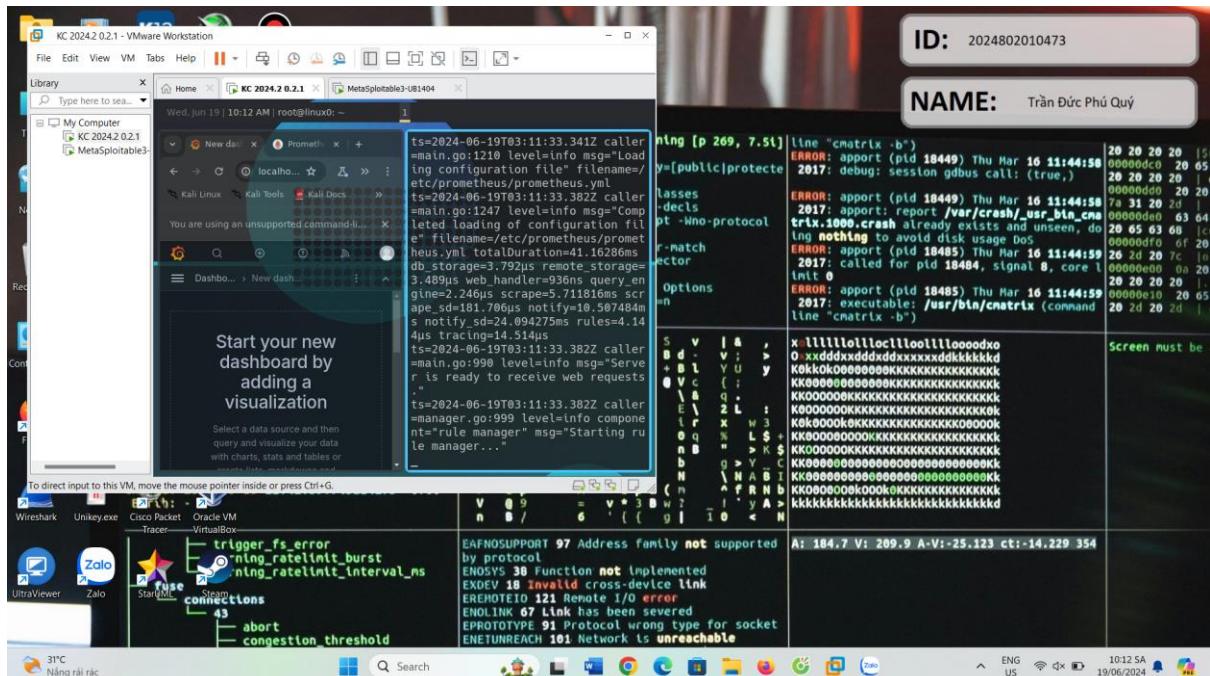
- B1:** Trên giao diện Dashboard ta kích vào “Add your first data source”, hoặc trên Menu trái ta chọn “**Connections -> Data sources**”
- B2:** Ta chọn **prometheus**, sau đó phần URL nhập “<http://localhost:9090>”, còn các cấu hình khác mặc định, sau đó nhấn “**Save & test**”. Hiện tại thấy hỗ trợ 152 kiểu **Data Source** khác nhau.

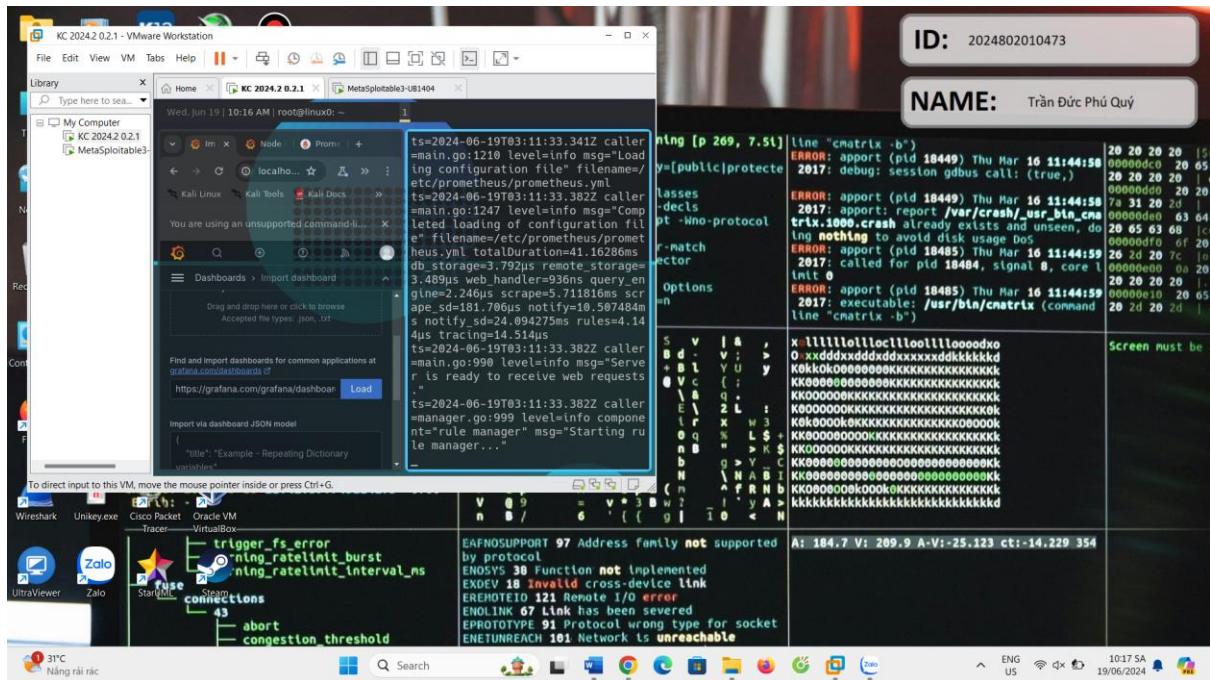




2. Tạo Dashboard để hiển thị dữ liệu:

- B1:** Trên giao diện Dashboard, ta kích vào “Create your first dashboard“, hoặc trên menu trái chọn “Dashboards -> New -> Import“. Việc tự tạo Dashboard hơi mất công nên ta sử dụng 1 trong các dashboard trên [Grafana Dashboards](#), có nhiều template đẹp, hiển thị thông tin khác nhau tùy mục đích sử dụng. Đã xem nhiều mẫu thích nhất mẫu **11074**, ta nhập ID **11074** vào rồi nhấn **Load**, sau đó bạn đổi tên và chọn **Data Source**, rồi nhấn nút **Import**.
- B2:** Sau khi Import thì vào lại giao diện để xem

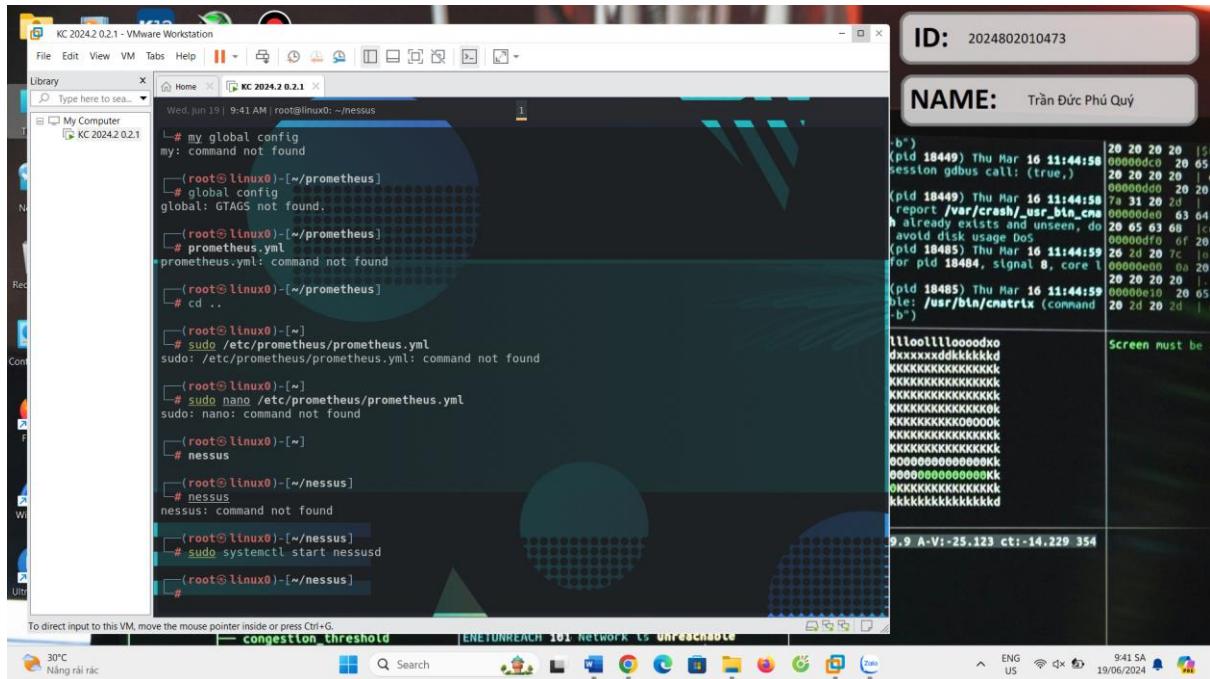




3. VULNERABILITY SCANNER - NESSUS (3D)

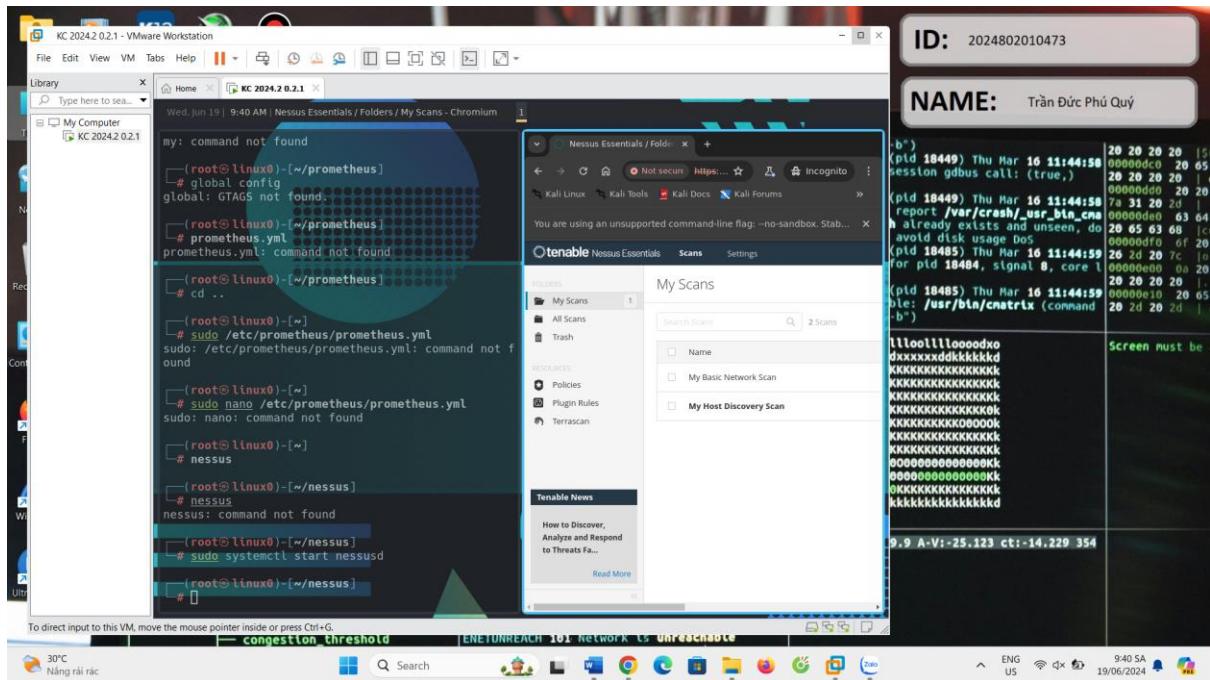
Trên Monitor, Đăng nhập với quyền root

3.1. Khởi chạy dịch vụ Nessus



Gợi ý: nessusd

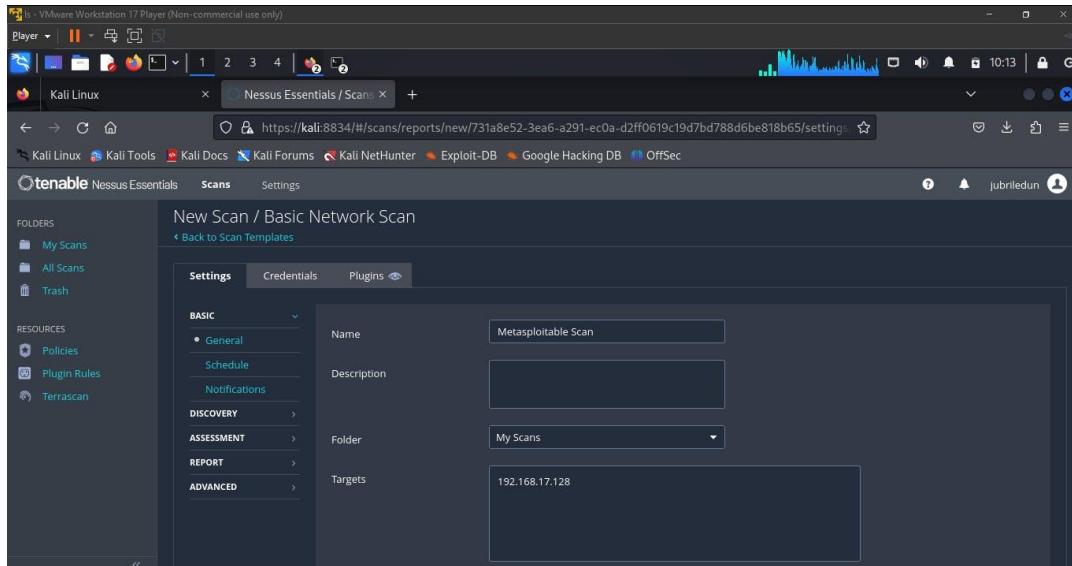
3.2. Truy cập giao diện web của nessus

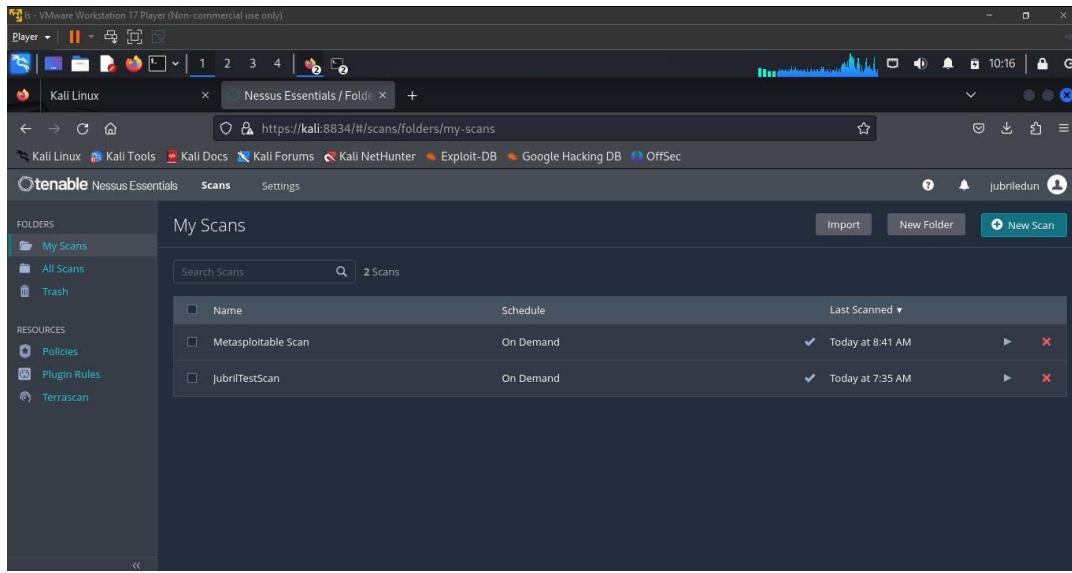


Gợi ý: port 8834

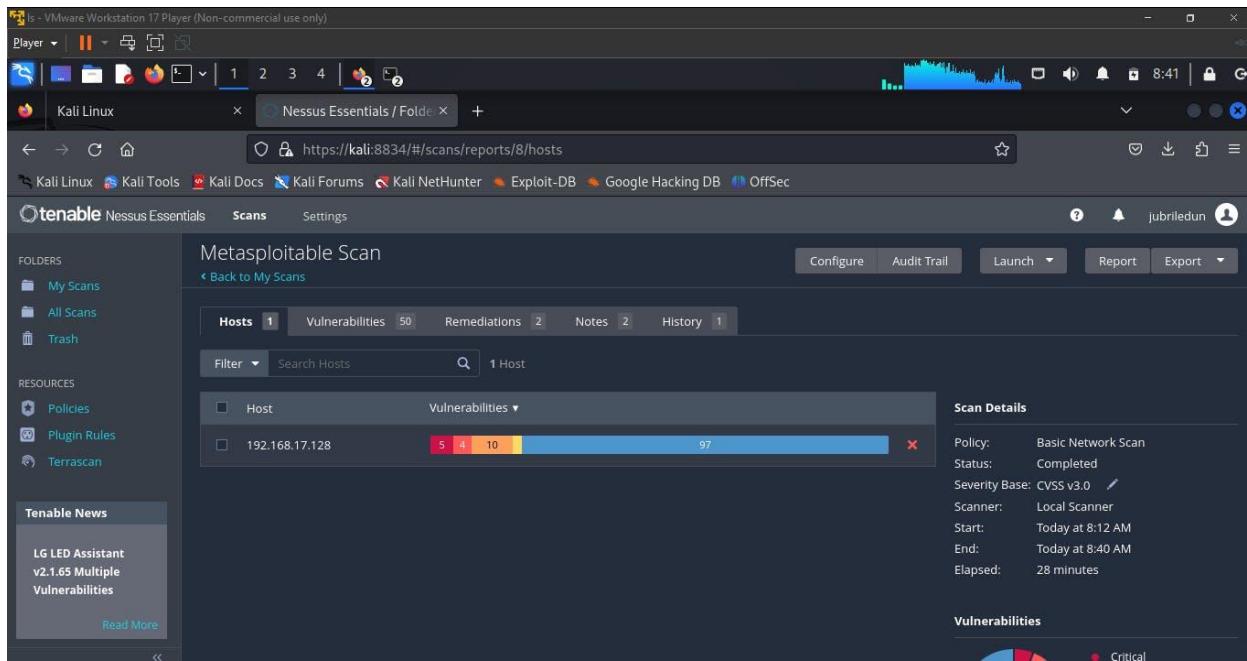
3.3. Thực hiện tương tự các thao tác bên dưới và chụp hình kết quả cuối cùng

"Policies < Scan Templates < Basic Network Scan ",





click the play button for Nessus to start scanning



after nessus finishes scanning the , click on "Vulnerabilities" to view the vulnerabilities found

