Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính nâng cao

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Kubernetes – Kube-hunter

GV: Nguyễn Duy

Ngày báo cáo: 27/04/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT534.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
3	Nguyễn Bình Thục Trâm	20520815	20520815@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 01: Kubernetes	100%	
2	Kịch bản 02: Kube-hunter	100%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Cấu hình máy thực hiện:

Intel core i5 8250U 8th gen

SSD 500GB

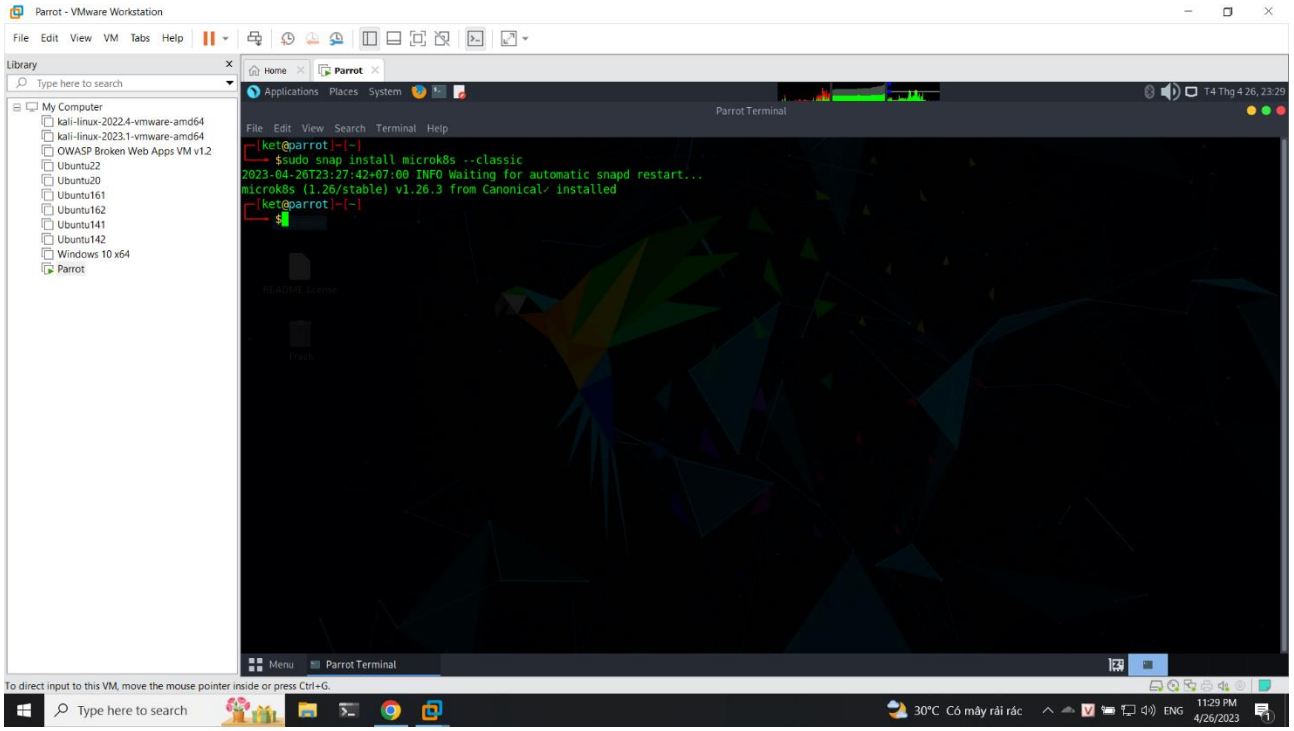
HDD 1000GB

RAM 16GB DDR3L

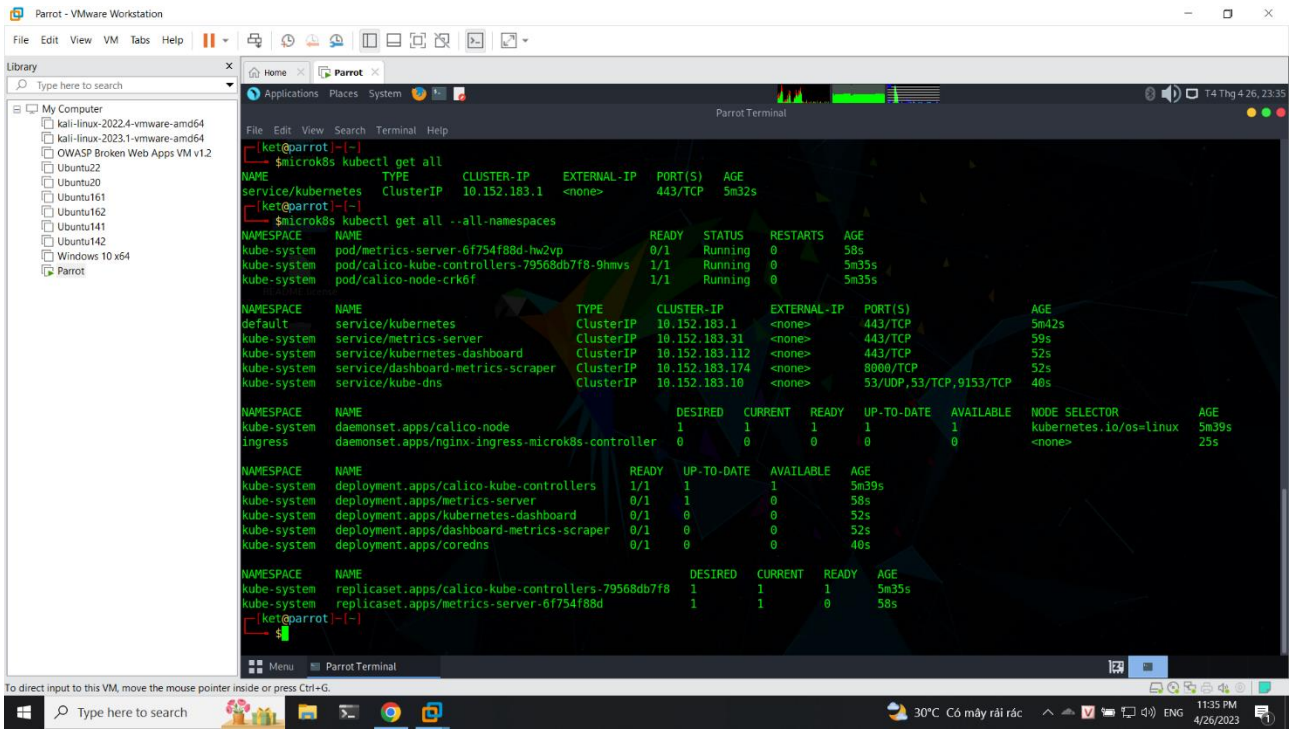
OS Parrot Linux 5.2 2023

2. Kịch bản 1

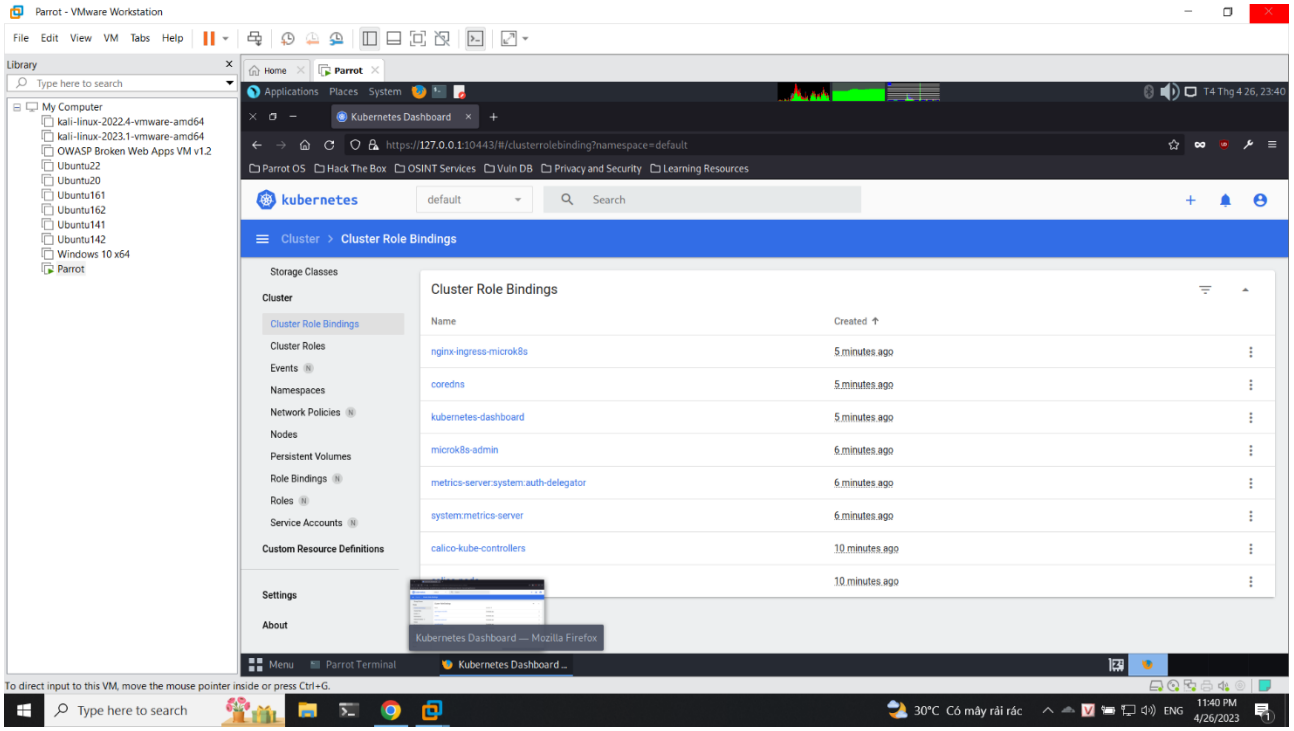
Thực hiện cài đặt Kubernetes thông qua snap (https://ubuntu.com/kubernetes/install)



Sau khi cài đặt và cấu hình xong ta sẽ có được các thông tin như bên dưới: Thông tin bao gồm các pod, service, daemon app, depolyment app



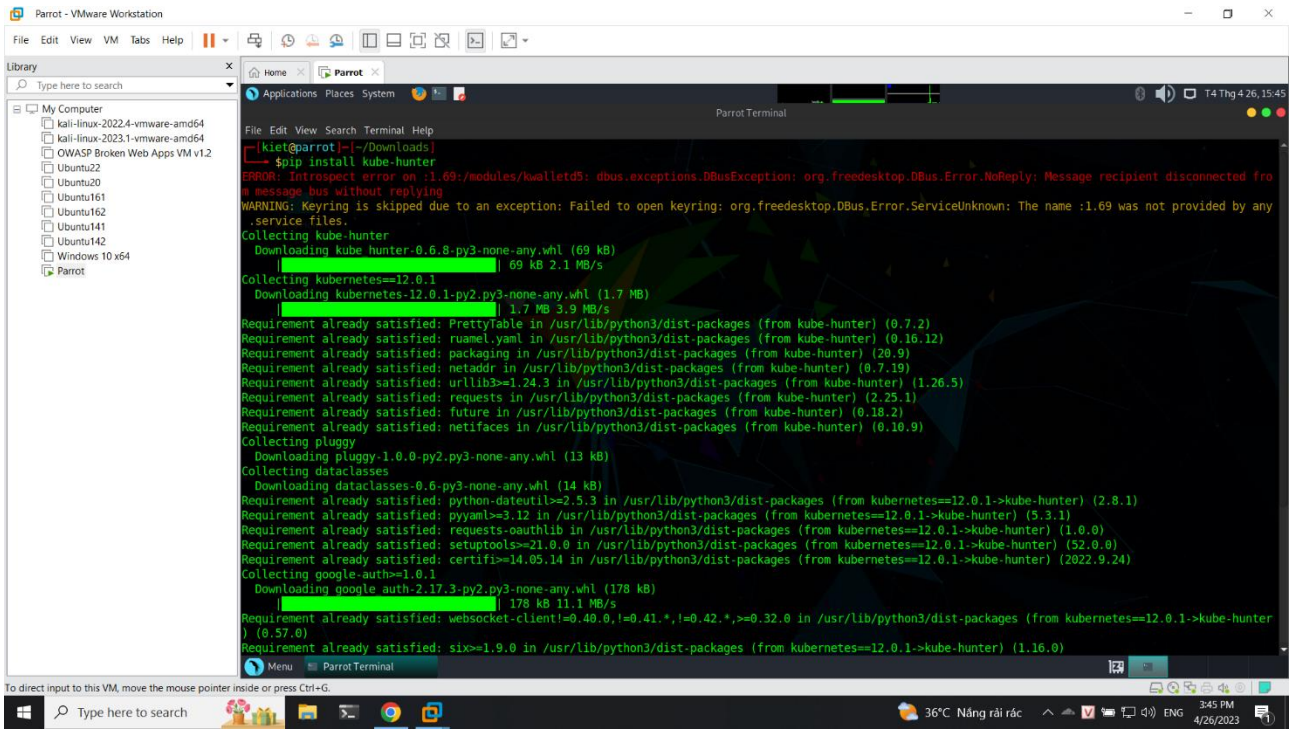
Ngoài ra ta có thể truy cập dashboard để xem các thông tin



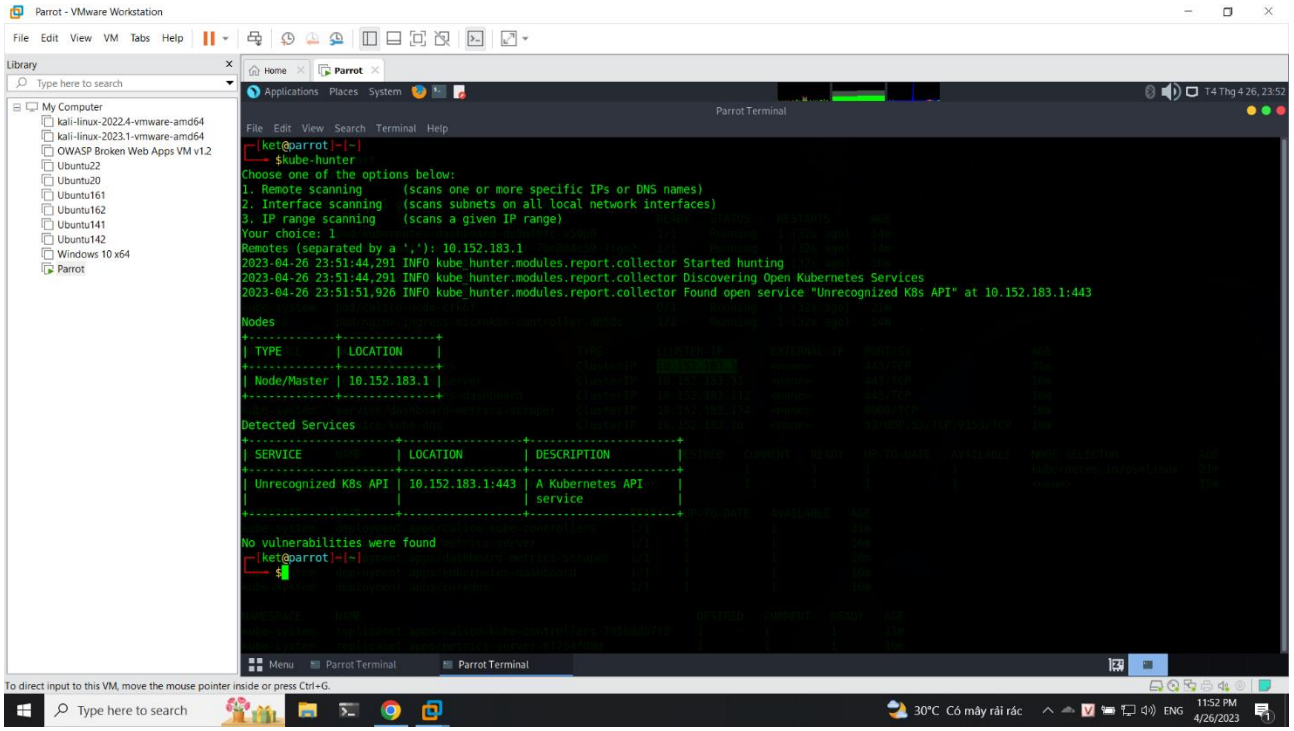
3. Kịch bản 2

Tham khảo: https://github.com/aquasecurity/kube-hunter

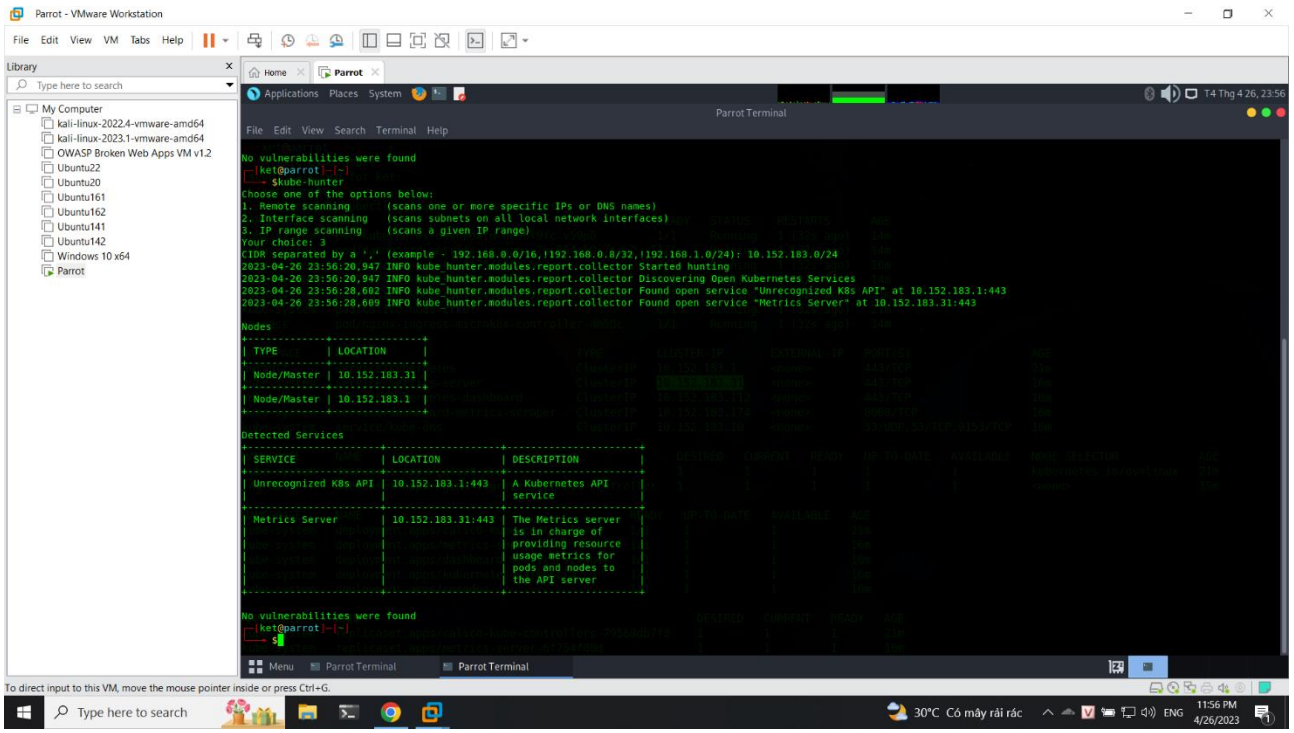
Đầu tiên ta sẽ cài đặt kube-hunter thông qua pip



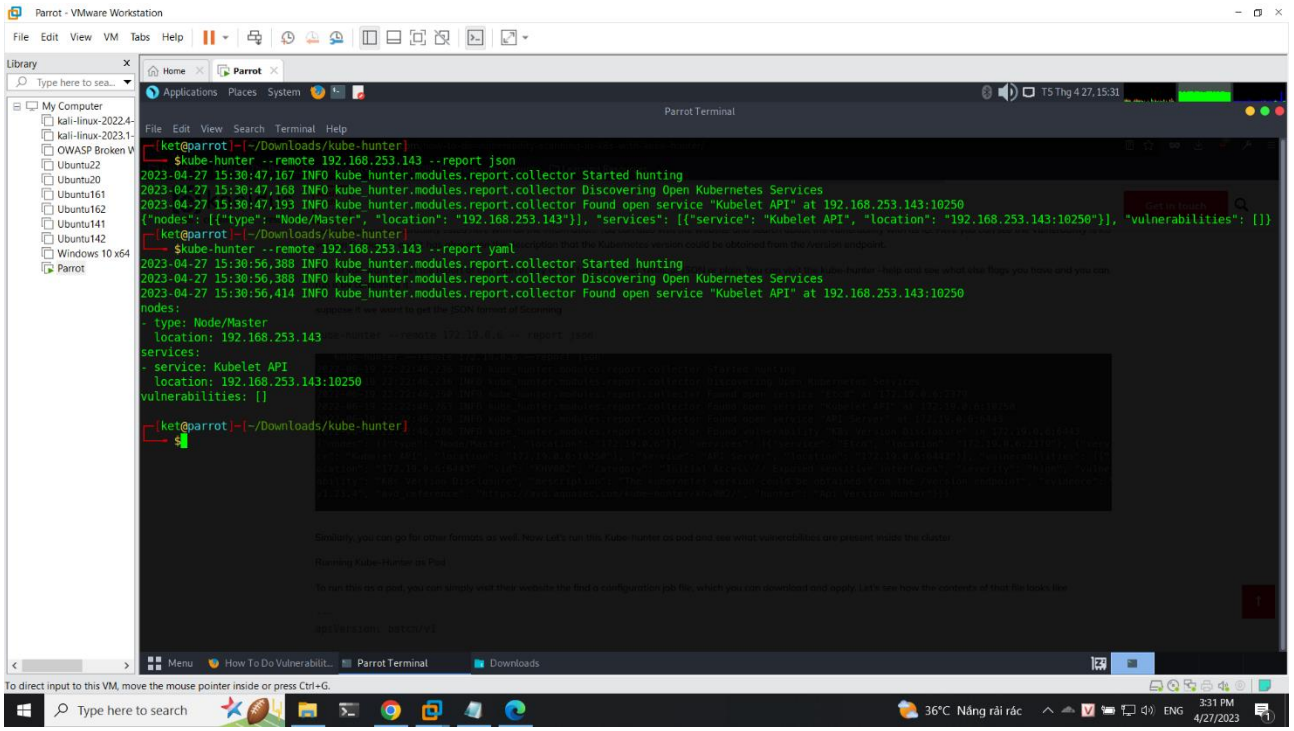
Chúng ta sẽ thử scanning theo ip



Tiếp tục ta sẽ scanning theo range ip



Ngoài ra sau khi kết quả thực hiện scan ta có thể thực hiện in kết quả report ra dạng json hoặc yaml



Ngoài ra ta thấy được là hiện tại ta chỉ đang scanning trên cluster mặc định nên không có lỗ hỏng, ở đây ta sẽ tạo thêm pod và job:

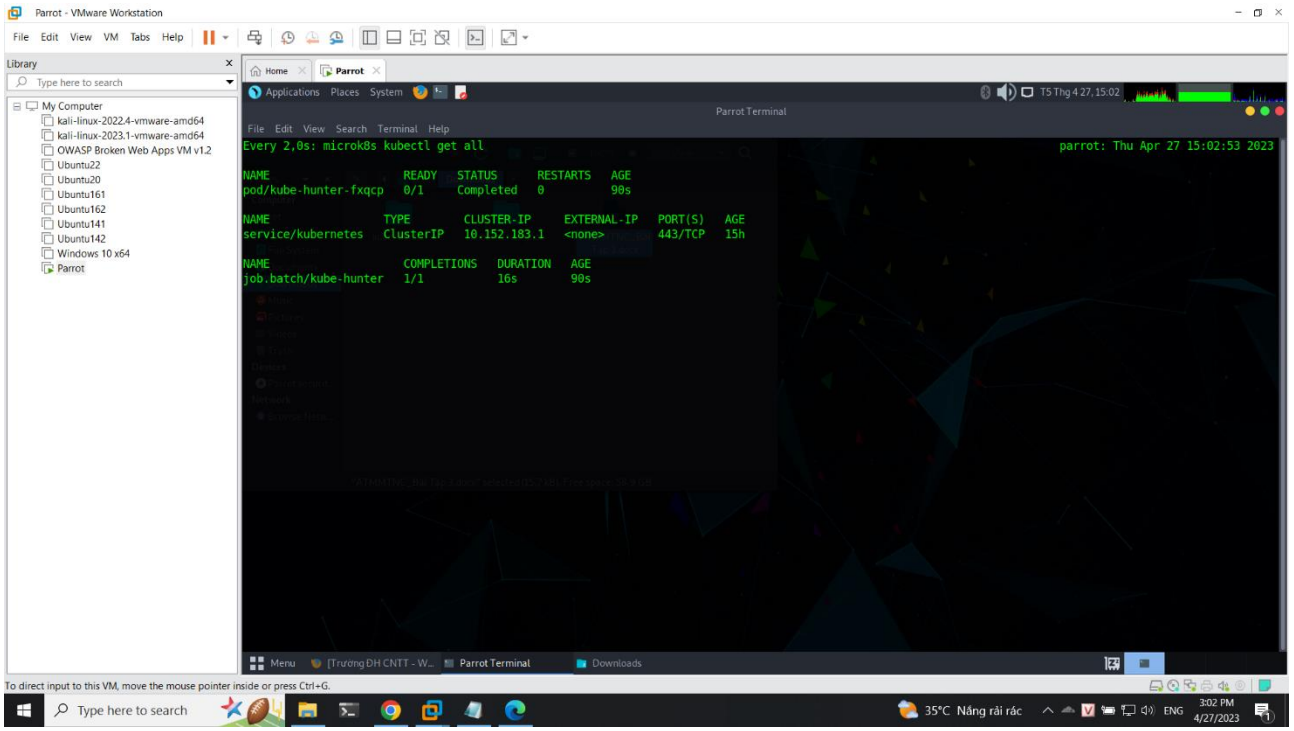
Với pod chứa các thông tin lỗ hỏng mà kube-hunter có thể scanning được

Với job là kube-hunter sẽ được tích hợp vào hệ thống kubernetes để phát hiện các lỗ hỏng và thông báo ngay trong logs

Thực hiện tạo thông qua job.yaml
(https://raw.githubusercontent.com/aquasecurity/kube-hunter/main/job.yaml)

```
┌──[ket@parrot]─[~/Downloads/kube-hunter]
└─$microk8s kubectl create -f ./job.yaml
E0427 14:36:39.423382   55061 memcache.go:287] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0427 14:36:39.435479   55061 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
job.batch/kube-hunter created
```

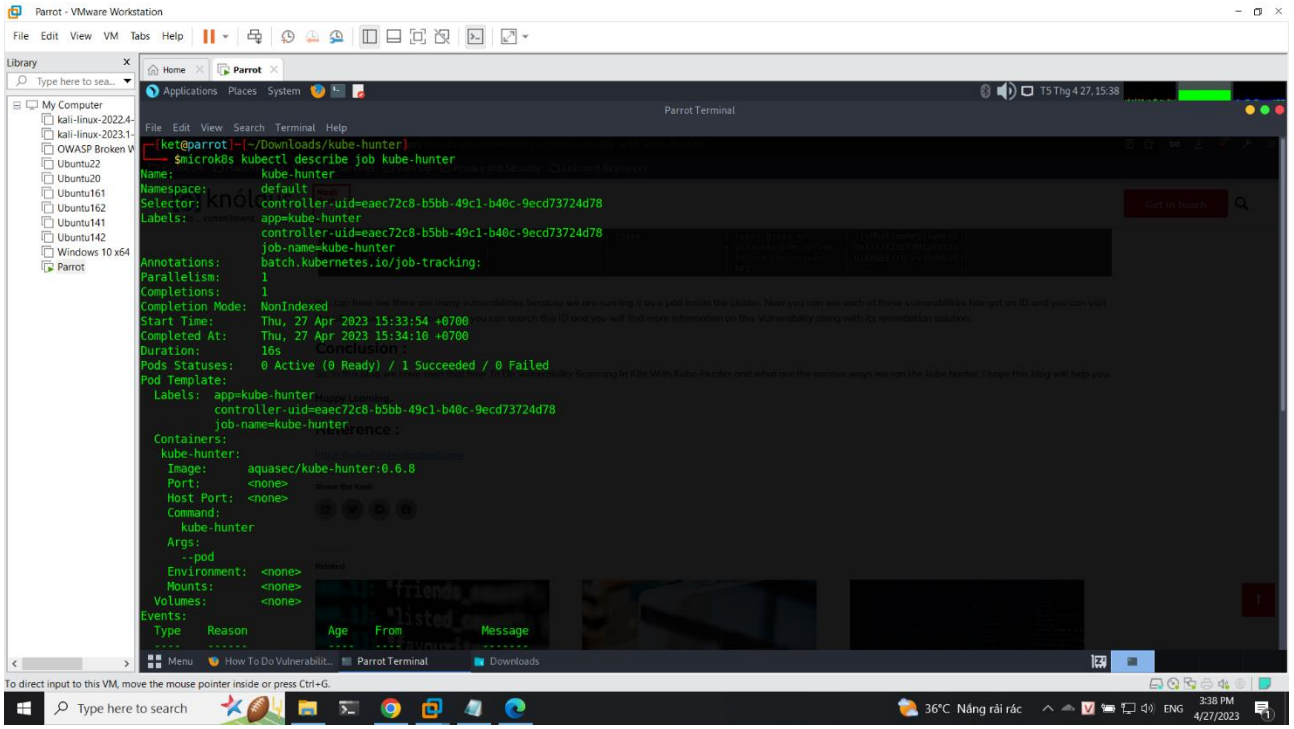
Thực hiện chạy



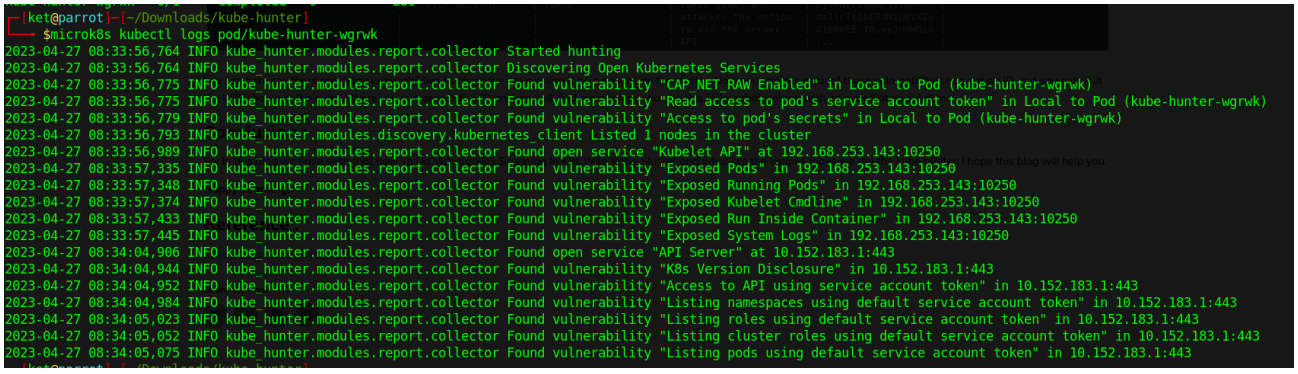
Sau khi chạy xong ta sẽ có thông tin namespace

```
┌──[✗]─[ket@parrot]─[~/Downloads/kube-hunter]
└─$microk8s kubectl get all --all-namespaces
NAMESPACE     NAME                                                READY   STATUS      RESTARTS       AGE
kube-system   pod/coredns-6f5f9b5d74-ncjtv                        1/1     Running     7 (2m3s ago)   15h
kube-system   pod/dashboard-metrics-scraper-7bc864c59-7tgn2       1/1     Running     7 (2m3s ago)   15h
kube-system   pod/kubernetes-dashboard-dc96f9fc-v59p8             1/1     Running     7 (2m3s ago)   15h
kube-system   pod/calico-kube-controllers-79568db7f8-9hmvs        1/1     Running     7 (2m3s ago)   15h
kube-system   pod/calico-node-crk6f                               1/1     Running     7 (2m3s ago)   15h
ingress       pod/nginx-ingress-microk8s-controller-db58c         1/1     Running     7 (2m3s ago)   15h
kube-system   pod/metrics-server-6f754f88d-hw2vp                  1/1     Running     7 (2m3s ago)   15h
default       pod/kube-hunter-6nk76                               0/1     Completed   0              45s

NAMESPACE     NAME                                TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)                  AGE
default       service/kubernetes                  ClusterIP   10.152.183.1     <none>        443/TCP                  15h
kube-system   service/metrics-server              ClusterIP   10.152.183.31    <none>        443/TCP                  15h
kube-system   service/kubernetes-dashboard        ClusterIP   10.152.183.112   <none>        443/TCP                  15h
kube-system   service/dashboard-metrics-scraper   ClusterIP   10.152.183.174   <none>        8000/TCP                 15h
kube-system   service/kube-dns                    ClusterIP   10.152.183.10    <none>        53/UDP,53/TCP,9153/TCP   15h

NAMESPACE     NAME                                        DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR            AGE
kube-system   daemonset.apps/calico-node                  1         1         1       1            1           kubernetes.io/os=linux   15h
ingress       daemonset.apps/nginx-ingress-microk8s-controller   1         1         1       1            1           <none>                   15h

NAMESPACE     NAME                                       READY   UP-TO-DATE   AVAILABLE   AGE
kube-system   deployment.apps/calico-kube-controllers    1/1     1            1           15h
kube-system   deployment.apps/metrics-server             1/1     1            1           15h
```

Ngoài ra ta có thể xem thông tin kube-hunter được tích hợp trong hệ thống



Cuối cùng ta sẽ thực hiện scanning



Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT