|  |  |
| --- | --- |
| Họ và tên | Huỳnh Ngọc Hân |
| Lớp | 10\_ĐH\_TMĐT |
| MSSV | 1050070035 |
| Bài tập | BT\_Thực hành buổi 1 |
| Môn | Bảo mật máy tính và hệ thống |

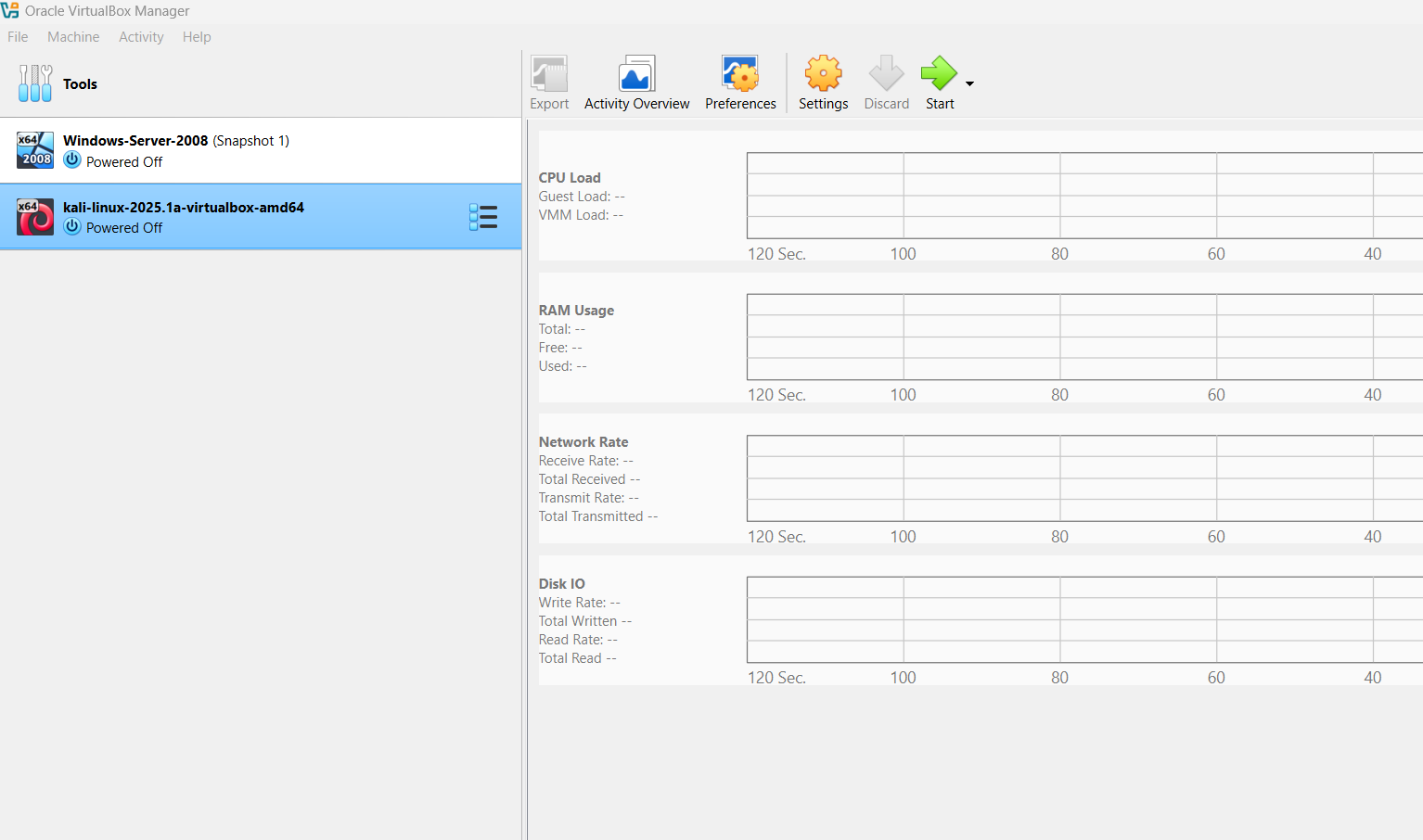
**Bài thực hành phục vụ cho nghiên cứu và học tập, không phục**

**vụ cho mục đích phá hoại và bất hợp pháp !**

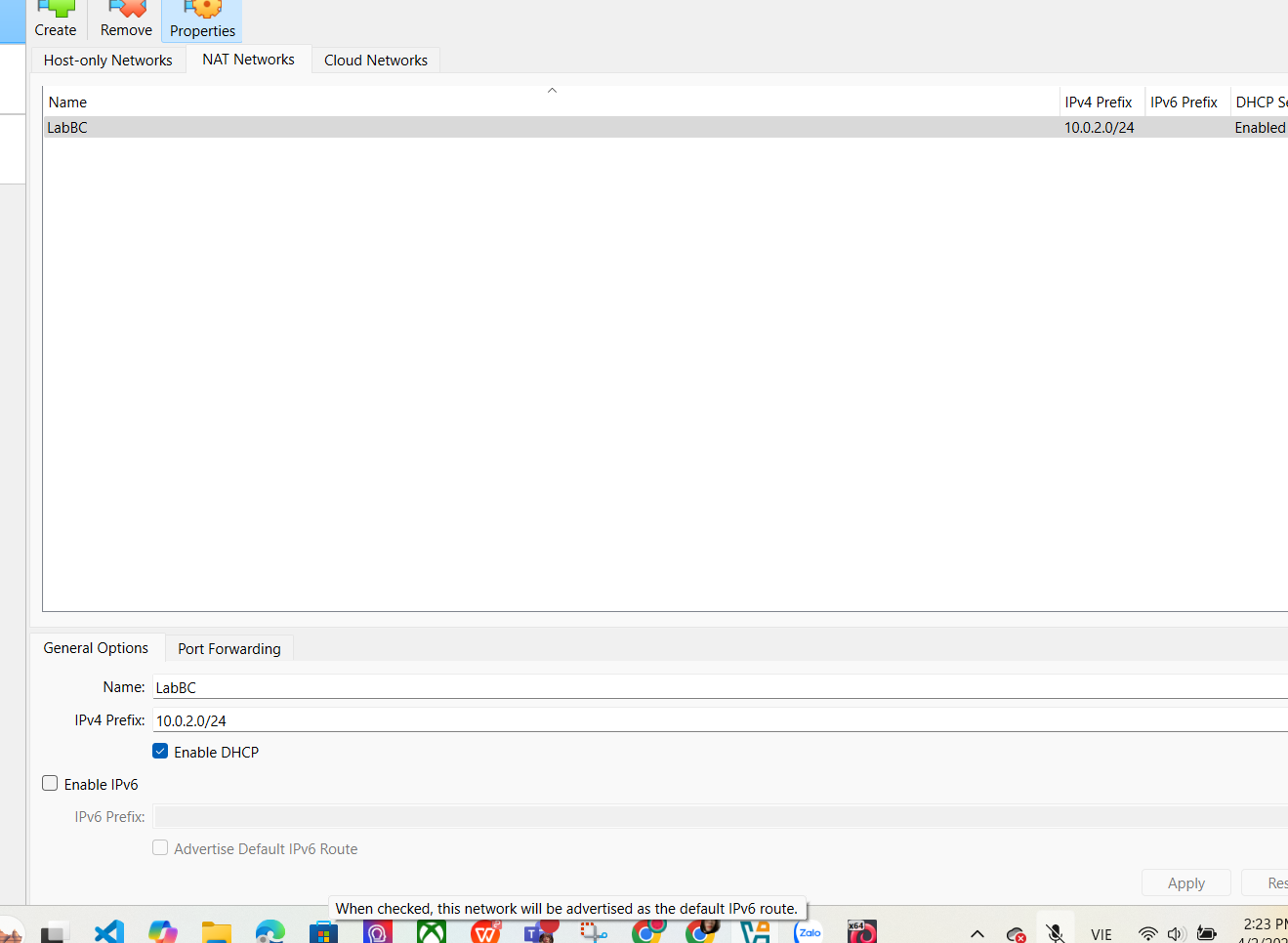
LAB1

Câu 1

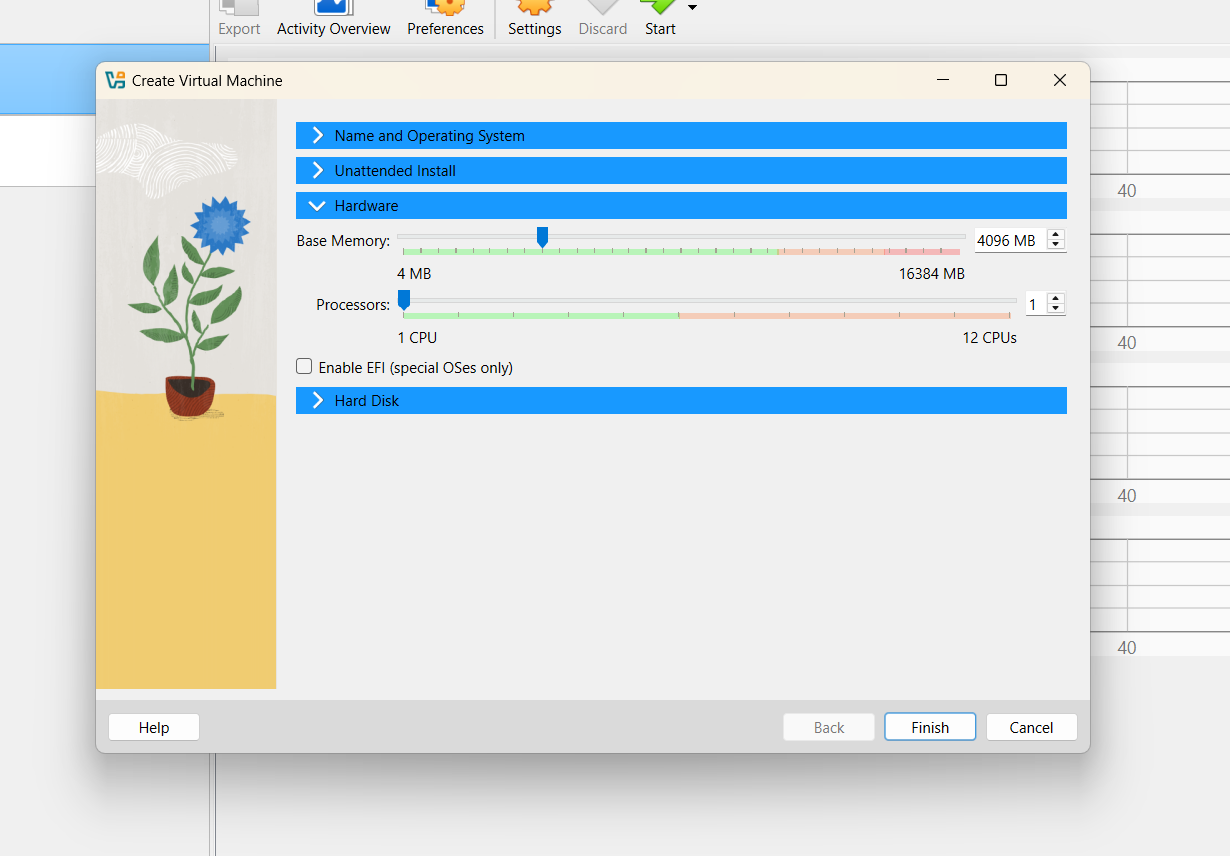
1. Cài đặt



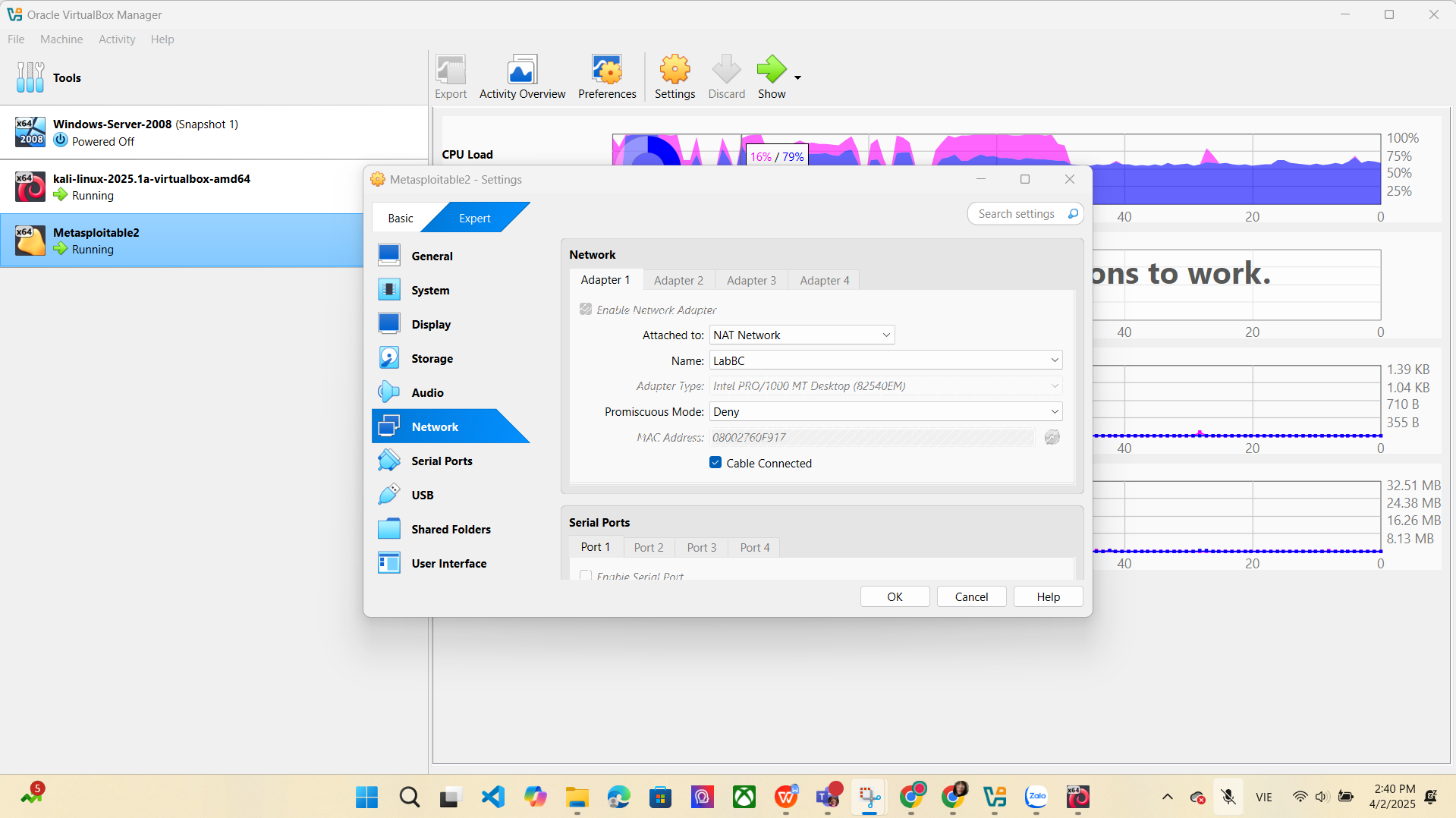
1. Đặt tên LABBC



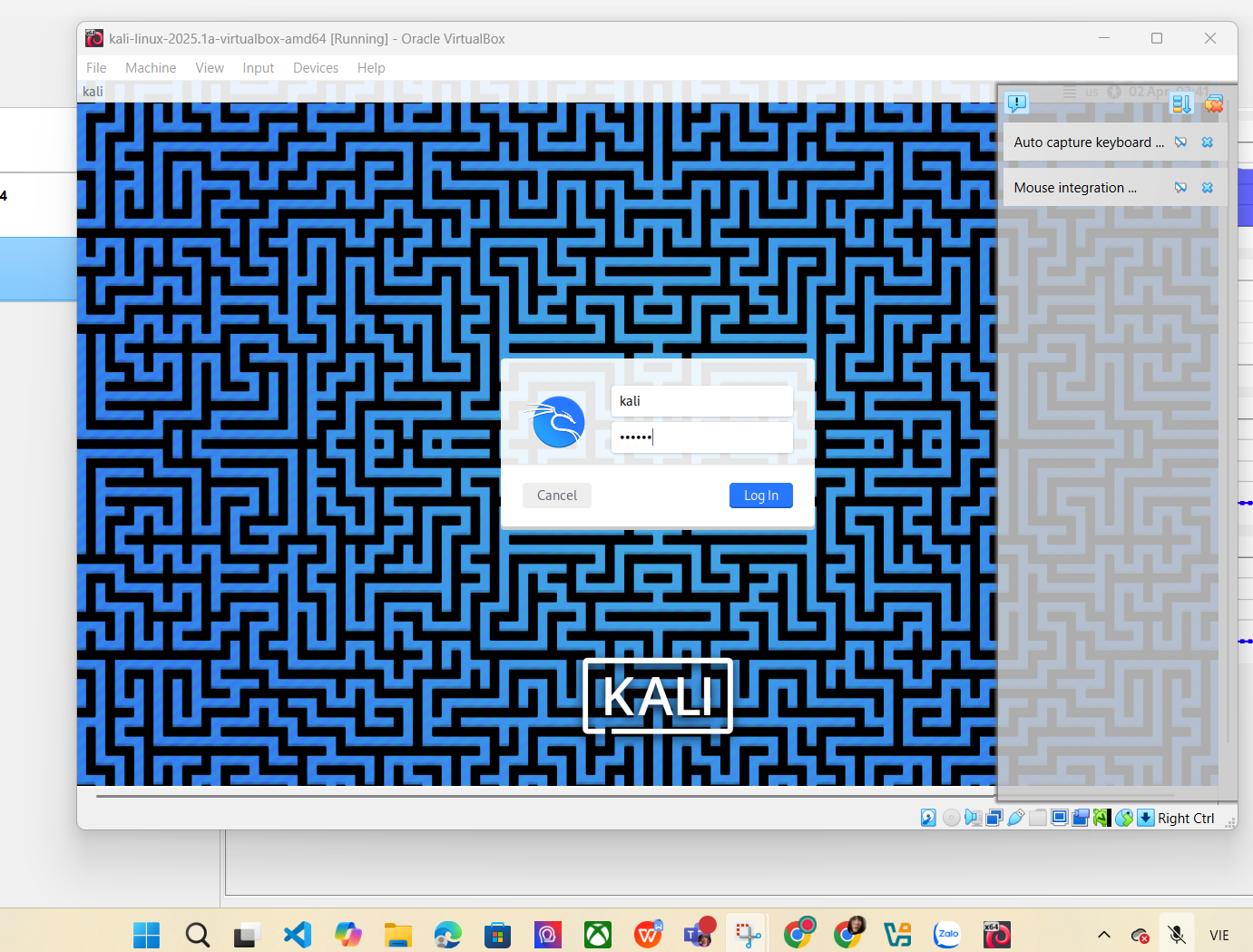
1. Metass



Đặt tên cho NatBC



1. Kali



Câu 2

### Chức năng chính của Nmap

Nmap (“Network Mapper”) là một tiện ích mã nguồn mở và miễn phí dùng để khám phá mạng và kiểm tra bảo mật. Nó hữu ích cho nhiều hệ thống và quản trị viên mạng trong các tác vụ như:

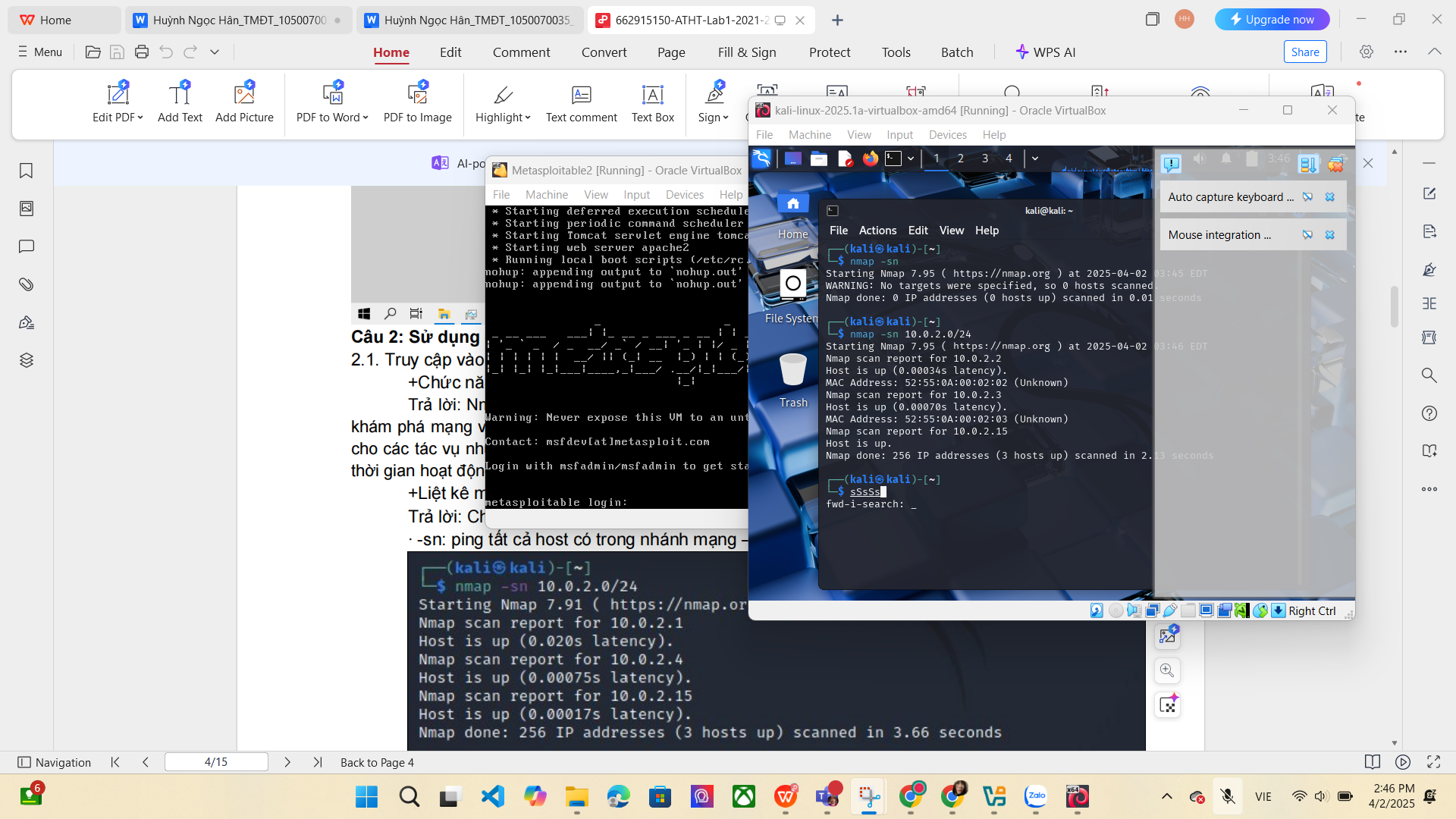
* Kiểm kê mạng
* Quản lý lịch nâng cấp dịch vụ
* Theo dõi máy chủ lưu trữ và thời gian hoạt động của dịch vụ

### Một số tham số trọng của Nmap

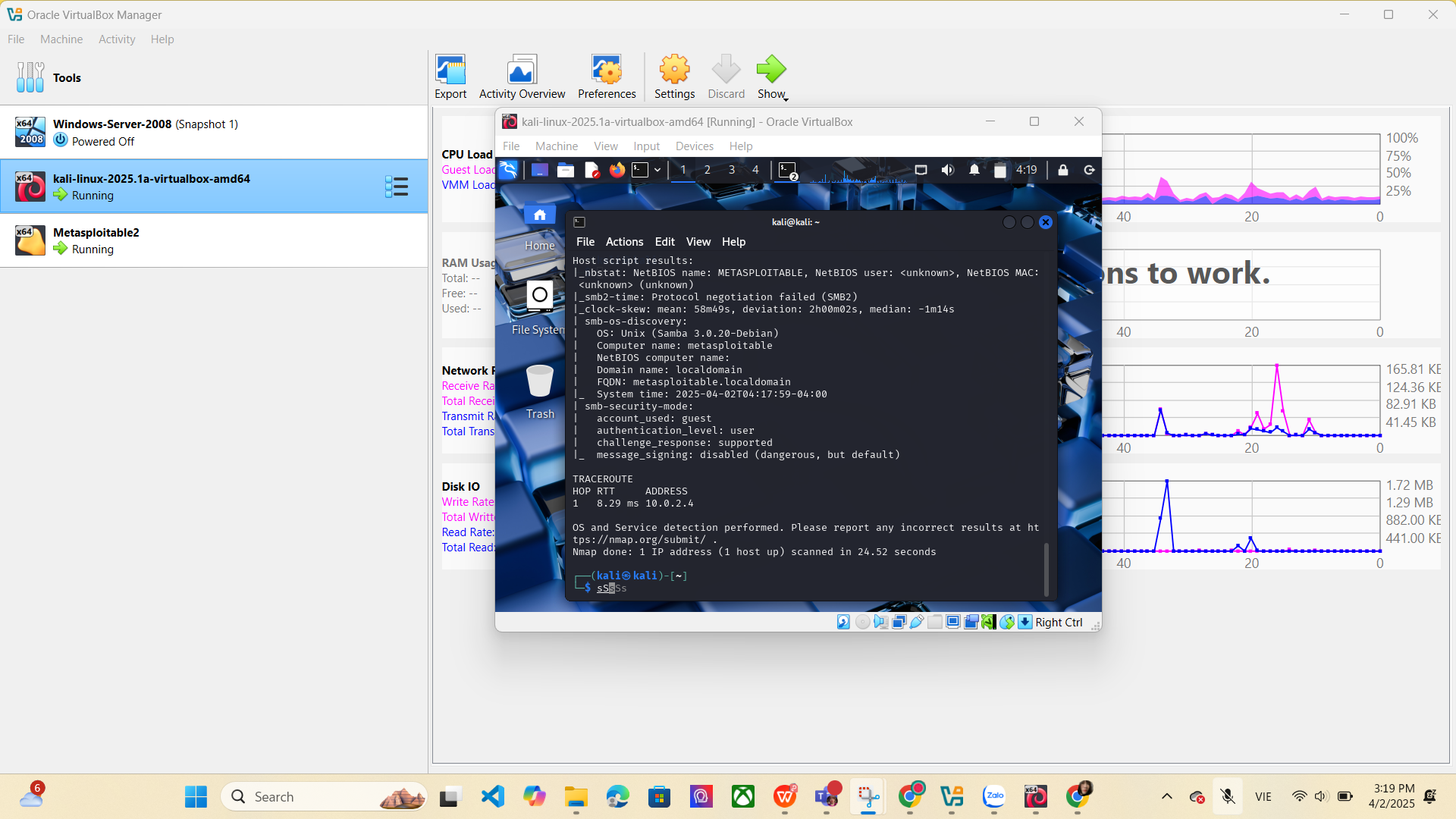
Dưới đây là một số tham số quan trọng của Nmap:

* -sn: Ping tất cả các host trong mạng mà không quét cổng.
* -sS: Quét SYN (Stealth scan).
* -sP: Quét ping để xác định host hoạt động.
* -p: Chỉ định cổng cụ thể để quét.
* -O: Nhận diện hệ điều hành của máy chủ.

-sn



-A



2.3. Tìm hiểu dịch vụ cài đặt trên cổng 21 của Metasploitable 2 có những lỗ hổng bảo mật gì?

\* Trả lời:

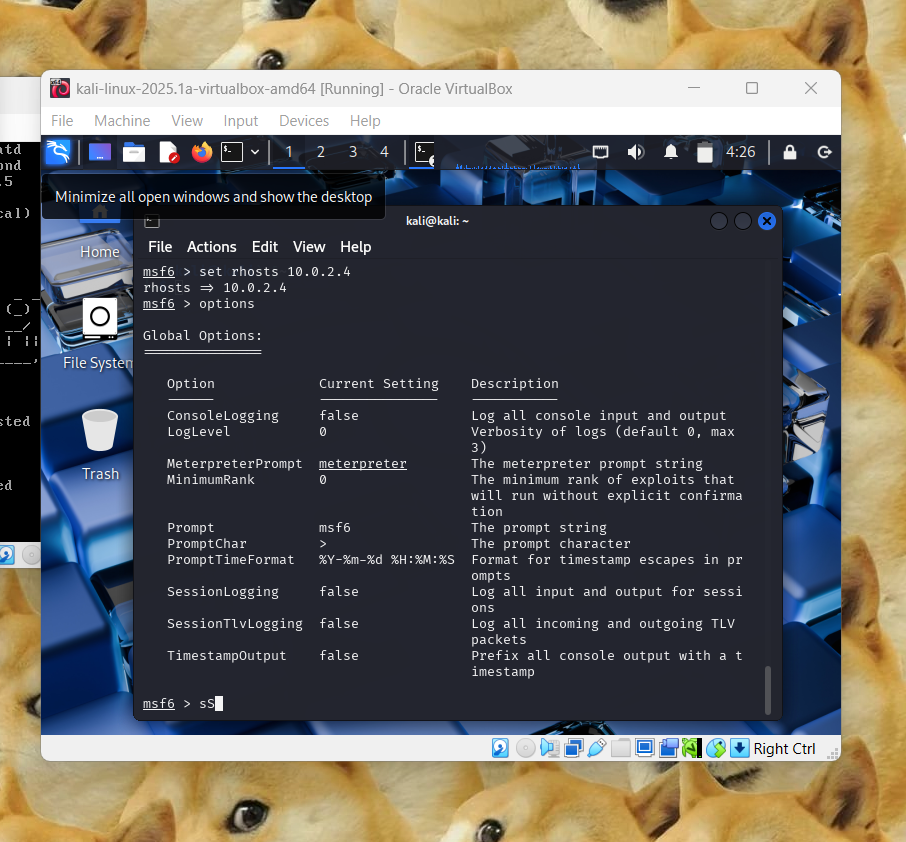
- Dịch vụ trên cổng 21 là open ftp và phần mềm của dịch vụ là vsftpd 2.3.4.

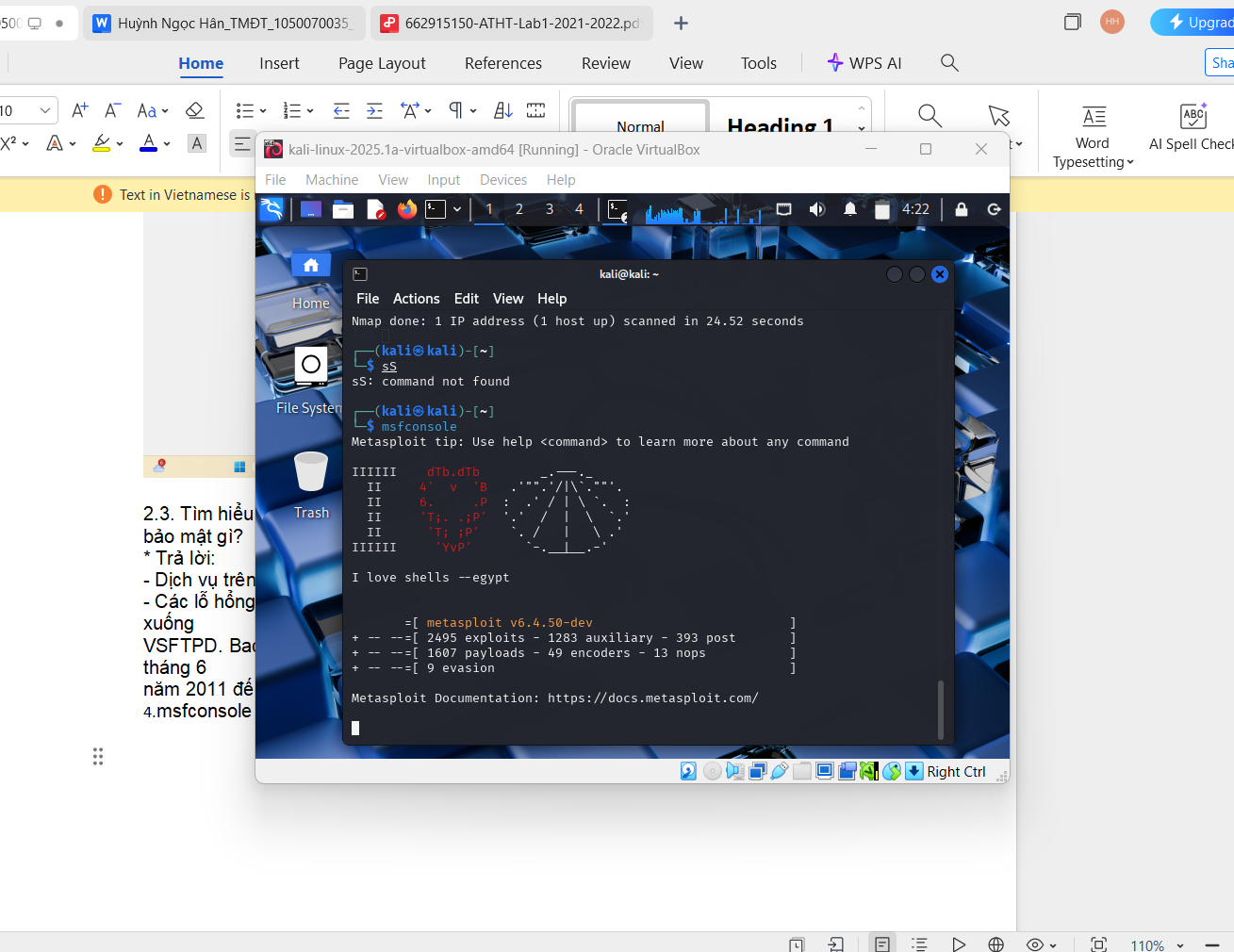
- Các lỗ hổng bảo mật: Một backdoor độc hại đã được thêm vào kho lưu trữ tải xuống

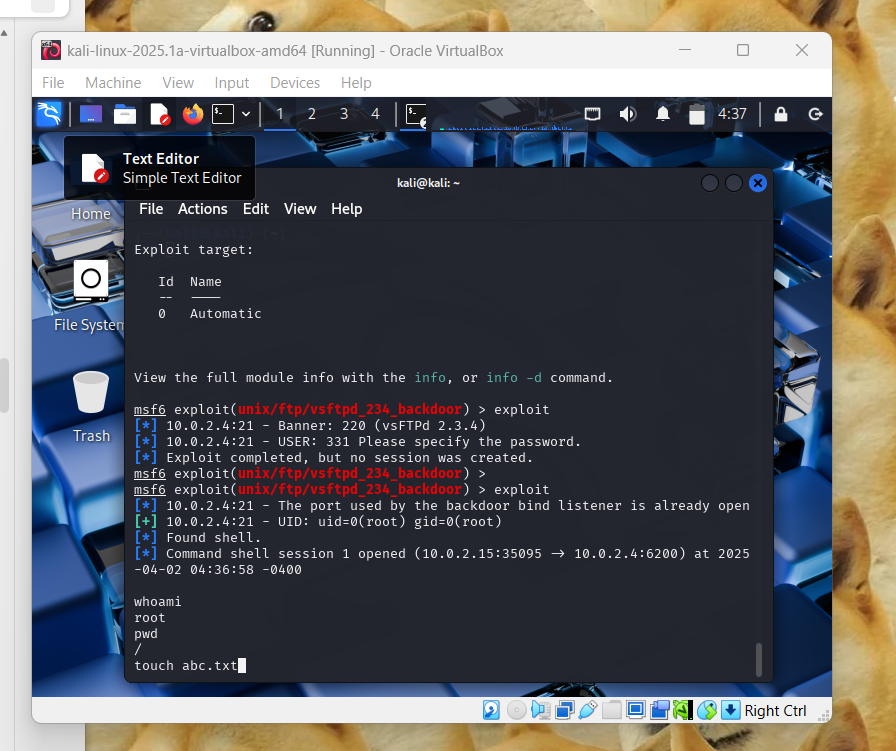
VSFTPD. Backdoor này đã được đưa vào kho lưu trữ vsftpd-2.3.4.tar.gz từ ngày 30 tháng 6

năm 2011 đến ngày 1 tháng 7 năm 2011 theo thông tin gần đây nhất có sẵn.

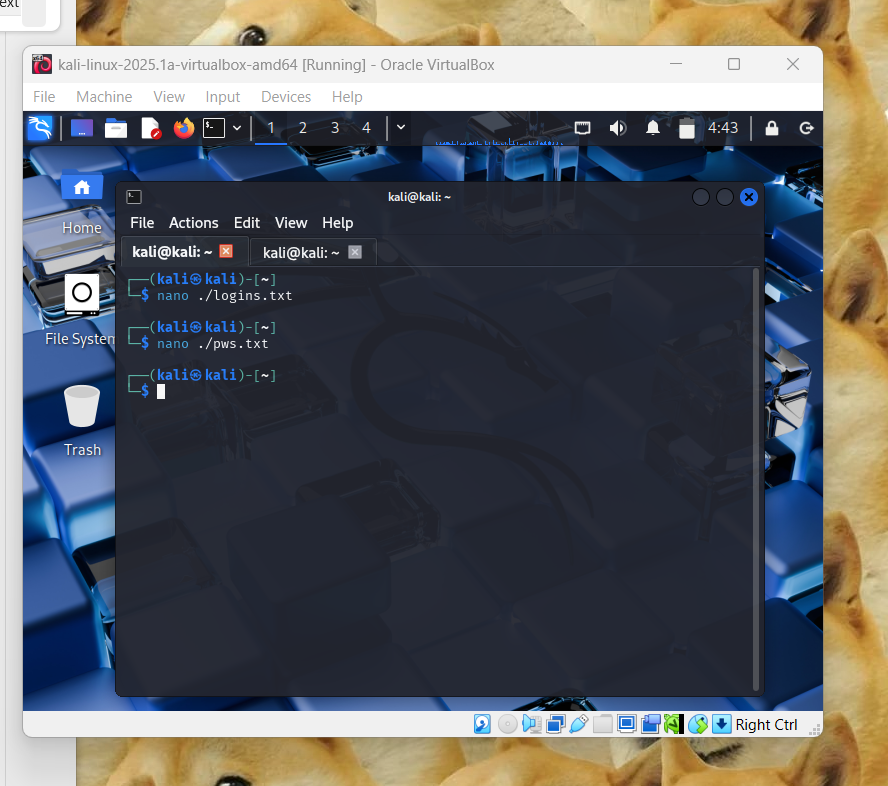
1. Msfconsole

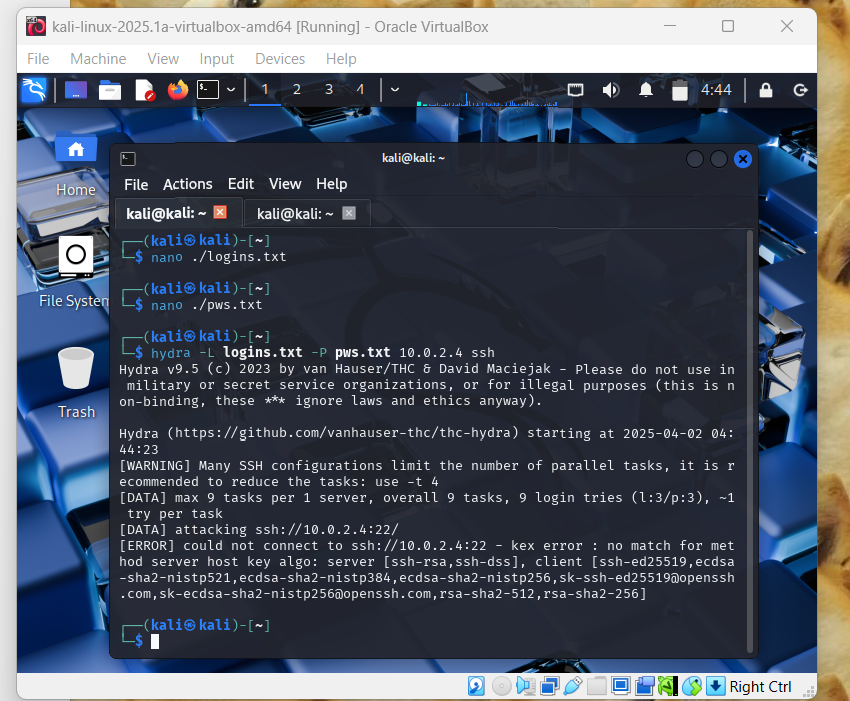






2.5





Câu 3:

