BÀI THỰC HÀNH SỐ 1

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lê Bảo Khánh**

**MSSV: 1911363**

**Nhóm: L01**

* + - * 1. **Tìm hiểu Kali Linux và các công cụ liên quan**
* Kali Linux là gì ?

Kali Linux là một bản phân phối Linux được phát triển và duy trì bởi Offensive Security khi được tổ chức này phát hành vào tháng 3 năm 2013, là sự thay thế phát triển cho hệ điều hành BackTrack. Offensive Security là một tổ chức nổi tiếng và đáng tin cậy trong thế giới bảo mật, thậm chí chứng nhận các chuyên gia bảo mật với một số chứng chỉ được xem trọng nhất hiện có như: OSCP, OSCE, OSWP, OSEE. Kali Linux là một hệ điều hành được sử dụng nhiều trong lĩnh vực bảo mật, bởi cả những hacker tìm cách xâm nhập hệ thống và những chuyên gia về bảo mật muốn bảo vệ các tài nguyên thông tin. Kali Linux cung cấp rất nhiều công cụ cho những tác vụ liên quan đến bảo mật.

* Hãy cho biết các nhóm công cụ liên quan hiện có trên Kali Linux:

1. Information Gathering

2. Vulnerability Analysis

3. Web Application Analysis

4. Database Assessment

5. Password Attacks

6. Wireless Attacks

7. Reverse Engineering

8. Exploitation Tools

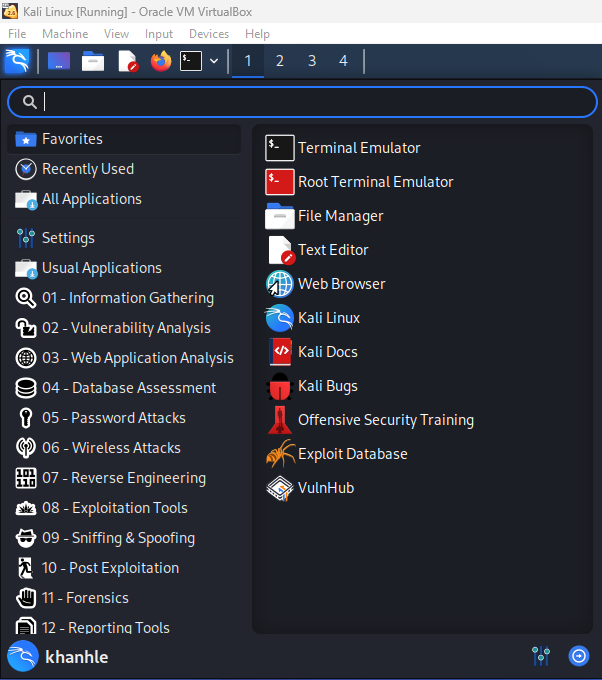
9. Sniffing & Spoofig

10. Post Exploitation

11. Forensics

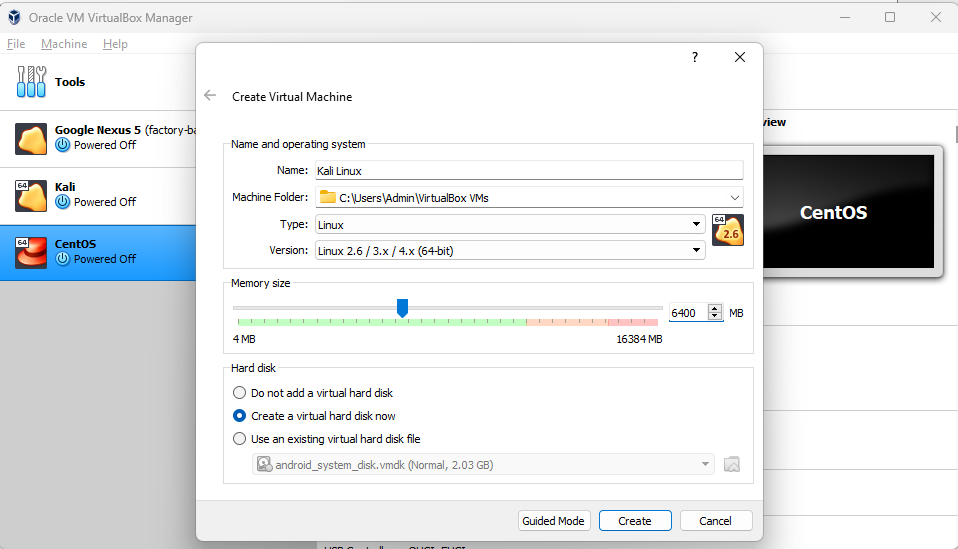
12. Reporting Tools

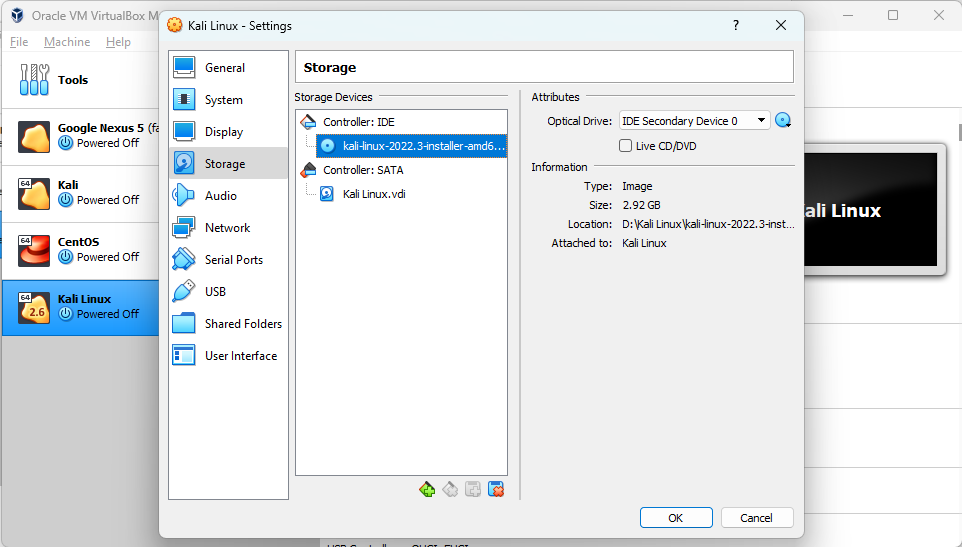
13. Social Engineering Tools



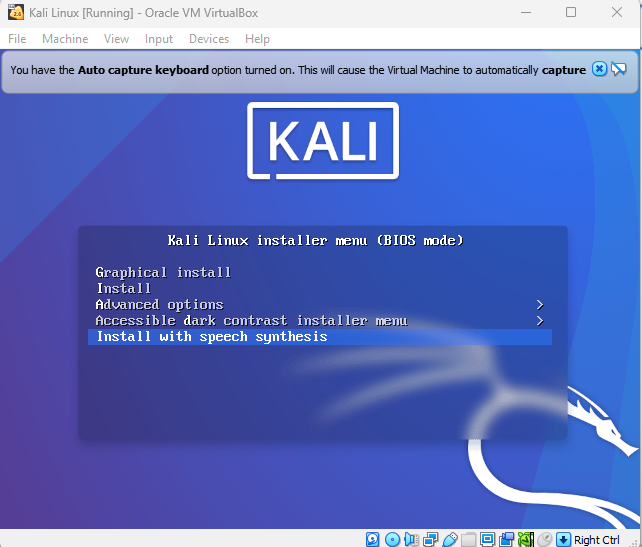
* + - * 1. **Cài đặt máy ảo Kali Linux**
* Cài đặt môi trường ảo hóa (Virtual Box). Hãy cho biết các bước và một số hình ảnh:
* Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh:

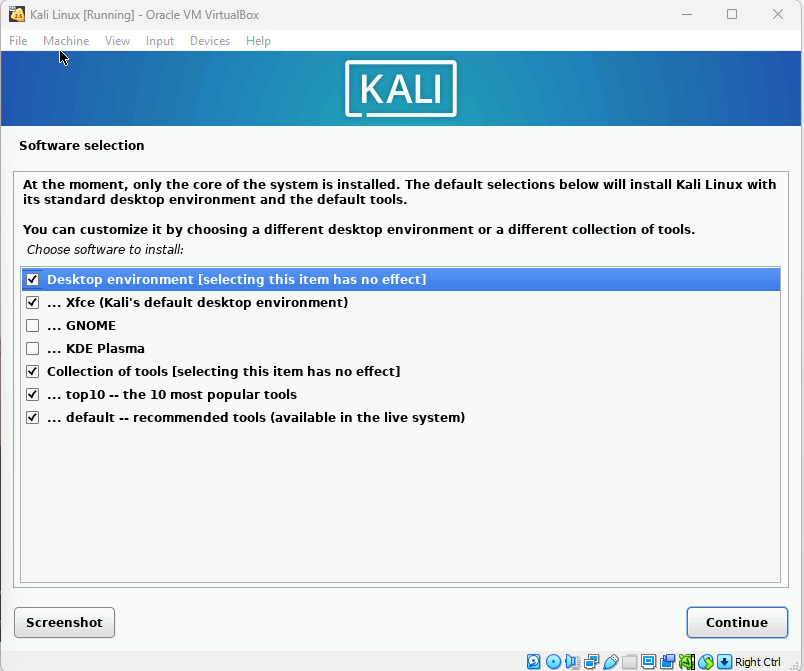
+ Tạo virtual machine



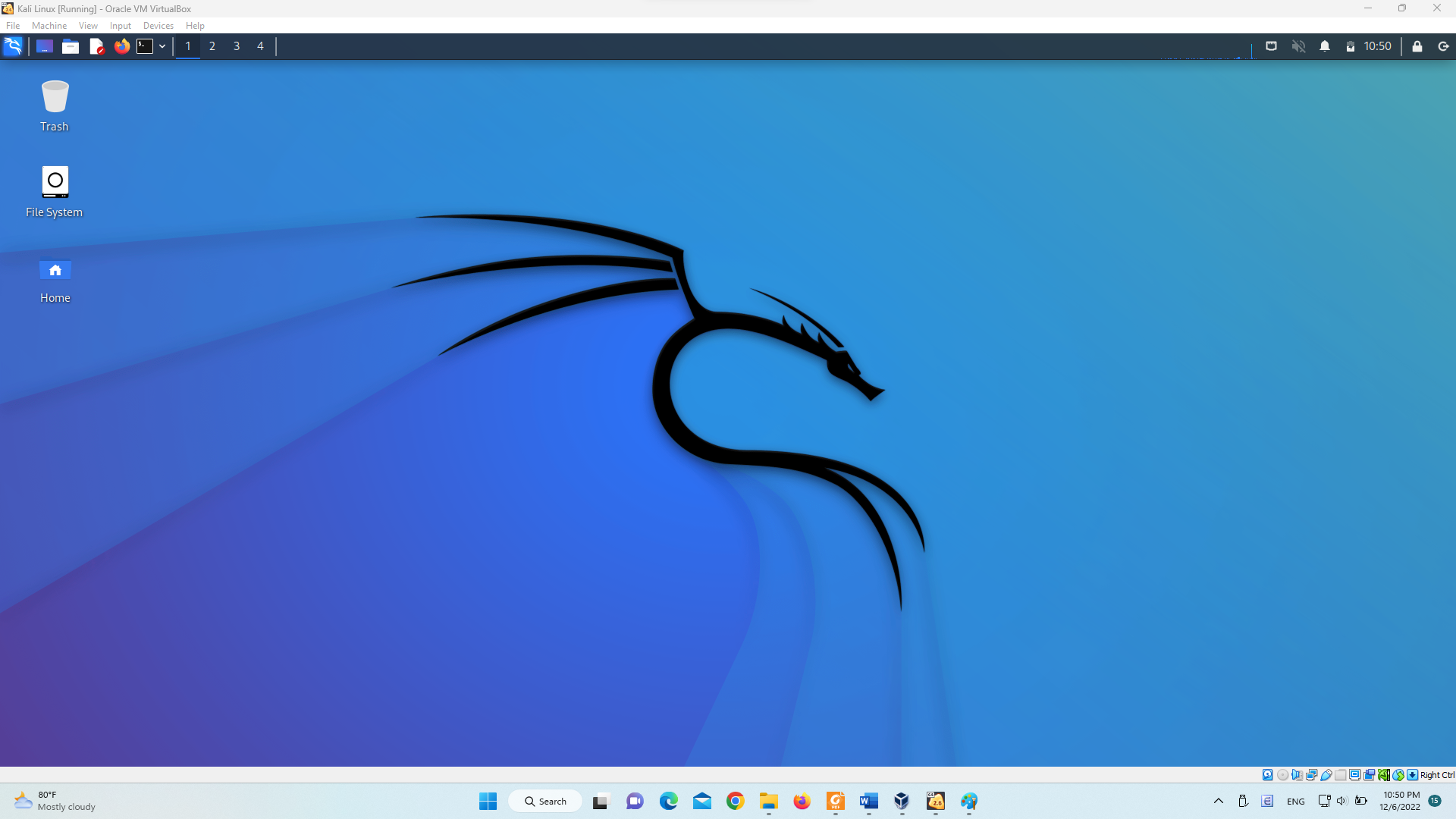


+ Cài đặt theo hướng dẫn



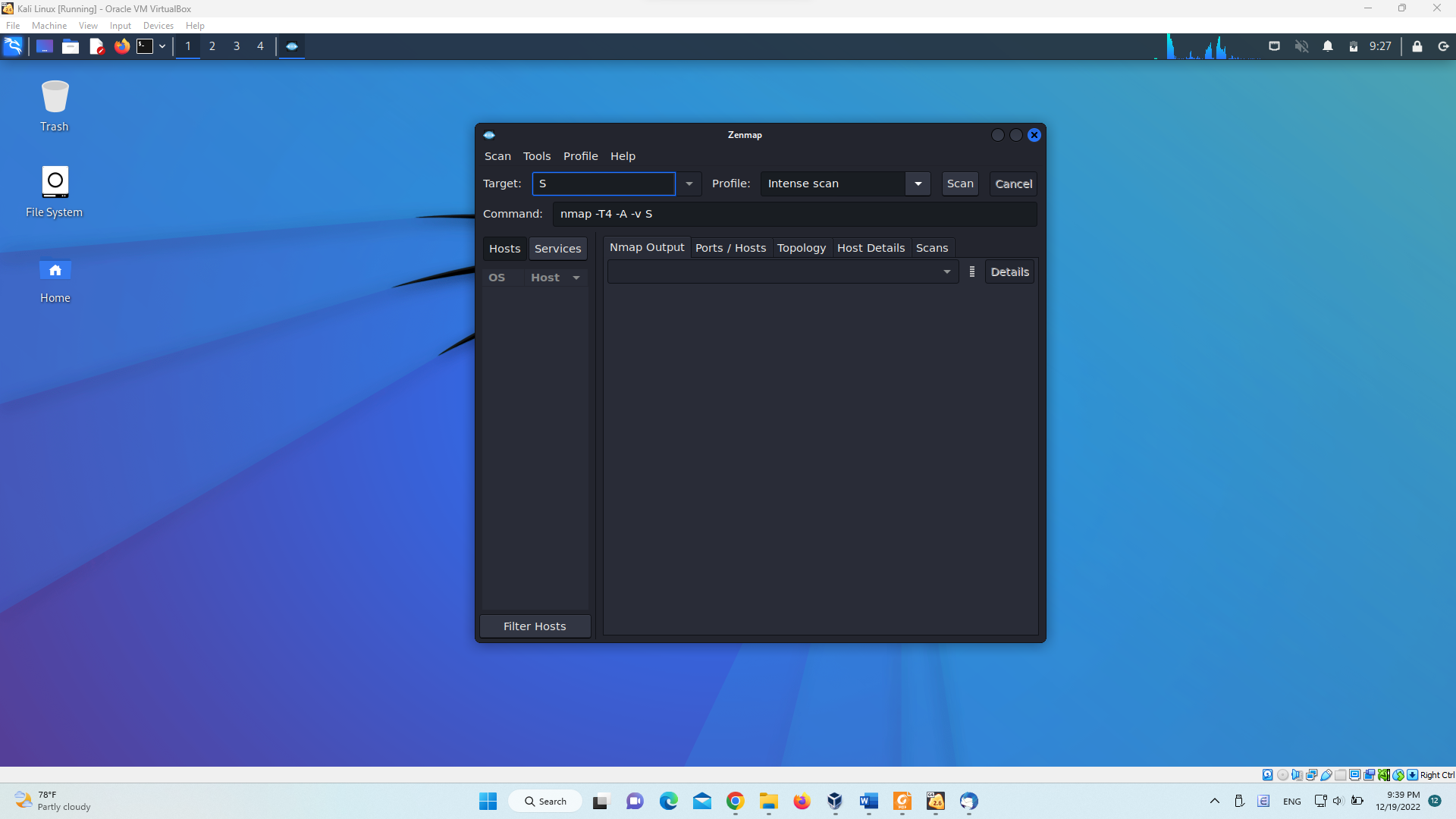


+ Kết quả

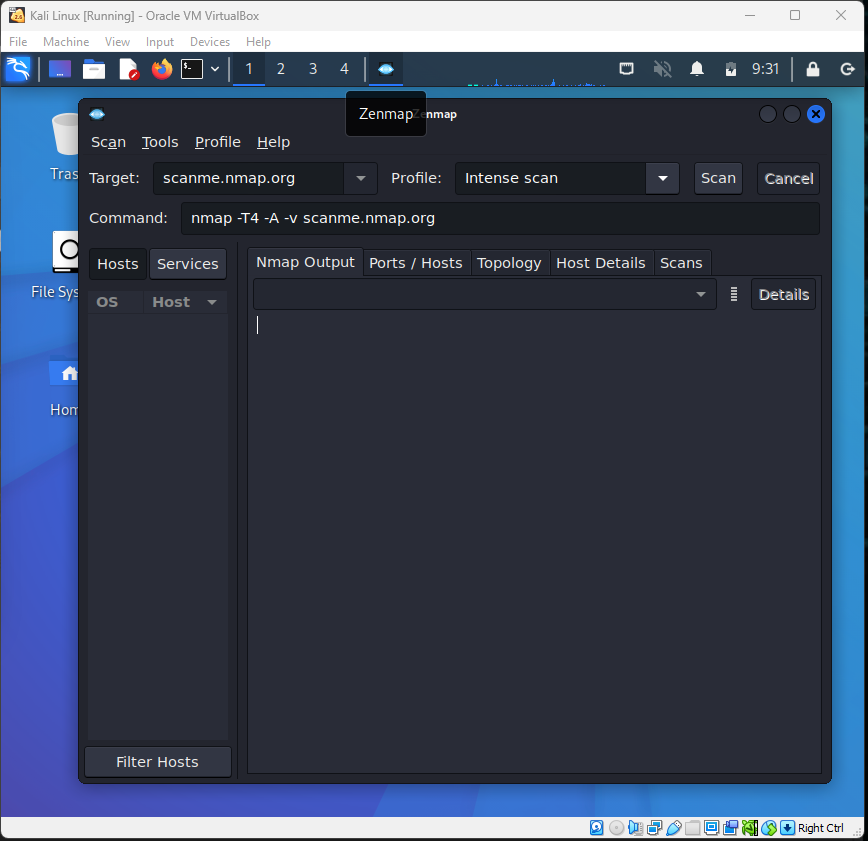


* + - * 1. **Thu thập thông tin mạng bằng cách quét mạng**
* Sử dụng công cụ [Nmap](https://tools.kali.org/information-gathering/nmap)/[Zenmap](https://www.linkedin.com/pulse/gui-based-nmap-zenmap-included-kali-linux-britto-sidhan). Hãy cho biết các bước và một số hình ảnh:

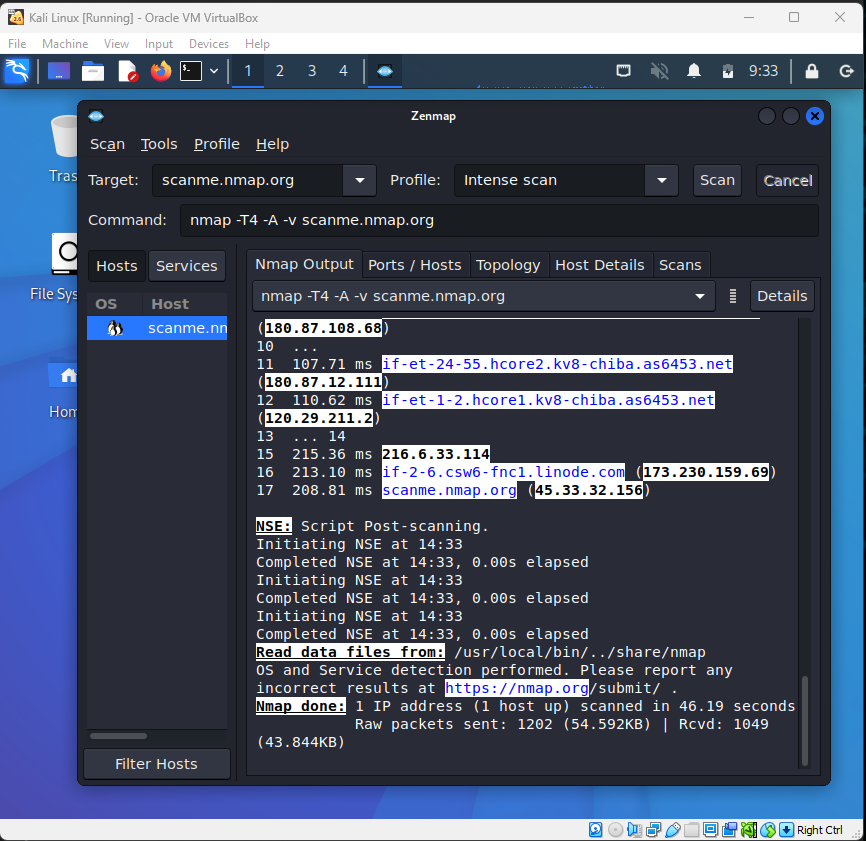
+ Khởi động Zenmap:



+ Chọn Target và Profile

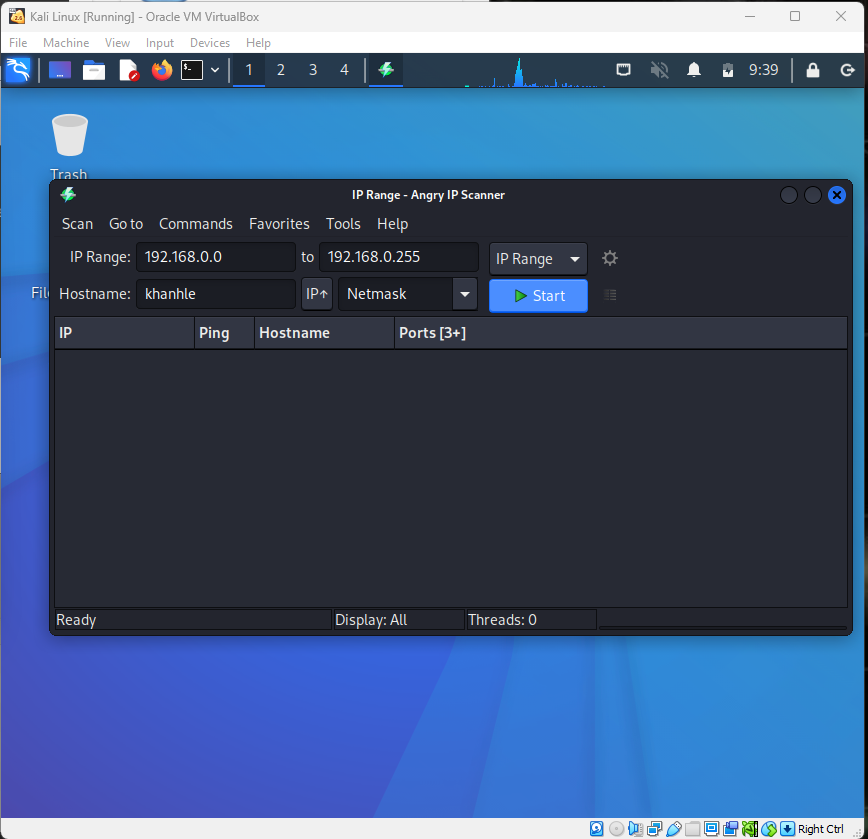


+ Bấm Scan

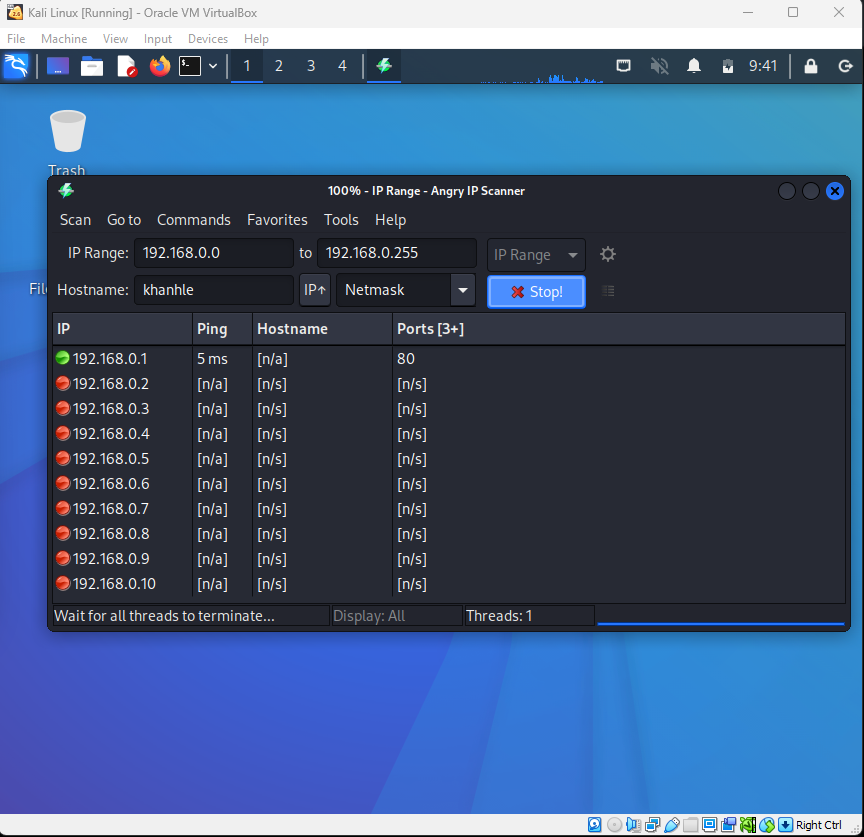


* Sử dụng [Angry IP Scanner](https://www.blackmoreops.com/2015/11/17/install-angry-ip-scanner-on-kali-linux/). Hãy cho biết các bước và một số hình ảnh:

+ Mở Angry IP Scanner



+ Bấm Start để bắt đầu Scan



* Đánh giá mức độ nguy hiểm của loại hình tấn công này:

+ Tấn công thụ động

+ Thu được các thông tin về hệ điều hành, các port đang mở, gói phần mềm

* Biện pháp đối phó đối với loại hình tấn công là gì ?

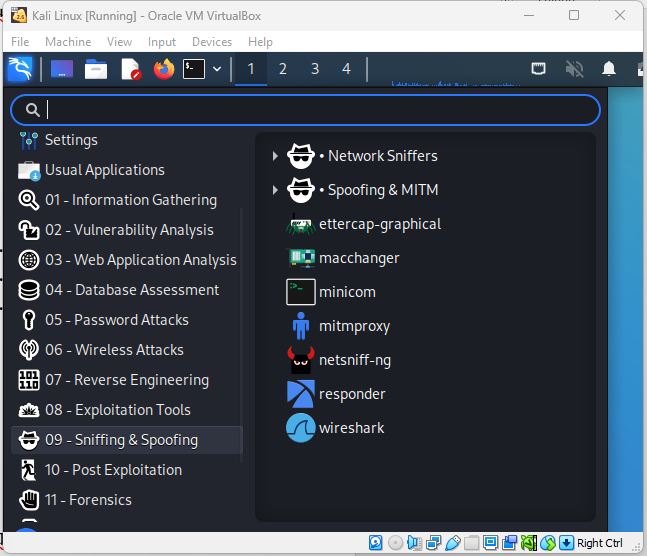
+ Không thể dung mã hóa

+ Phát hiện xâm nhập bất hợp pháp: Nếu dò quét mạng xảy ra thì phải chặn ngay

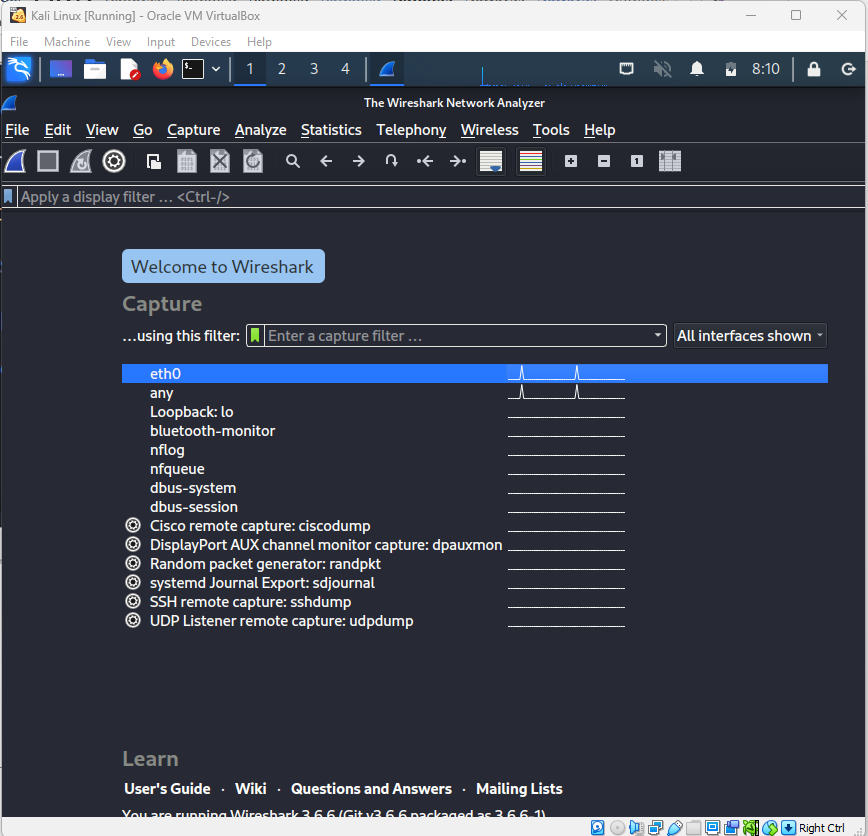
+ Các hệ điều hành, phần mềm quan trọng thì phải biên dịch lại -> che dấu thông tin nhạy cảm (tên hệ điều hành, gói phần mềm, version…)

* + - * 1. **Nghe lén thông tin, dữ liệu**
* Dùng Wireshark để bắt gói, phân tích gói tin bắt được. Hãy cho biết các bước và một số hình ảnh:

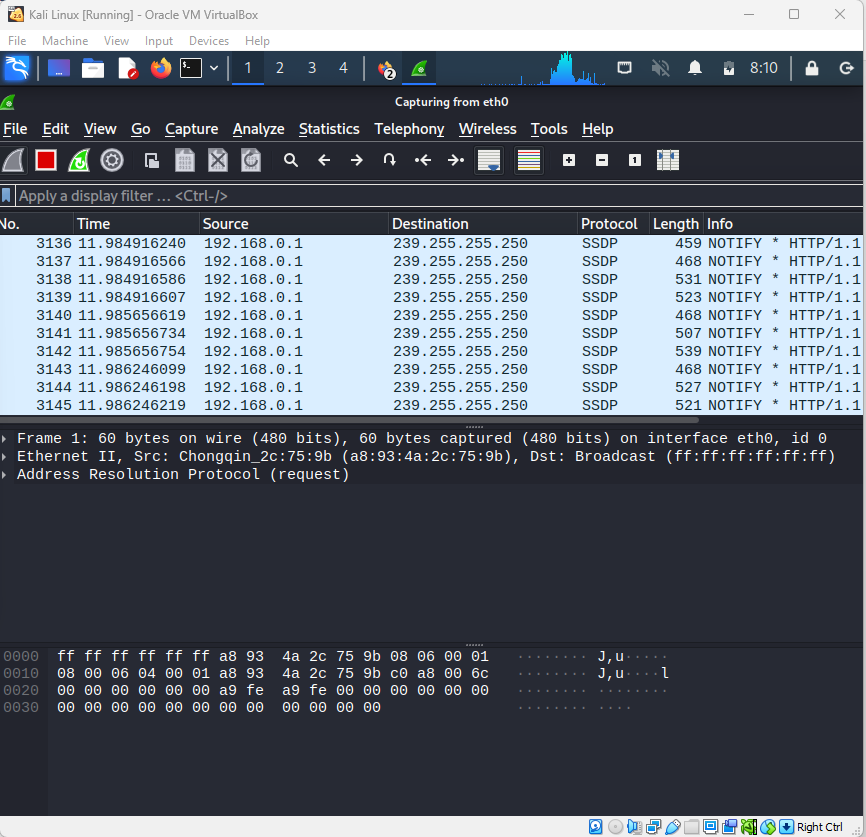
+ Khởi động Wireshark:



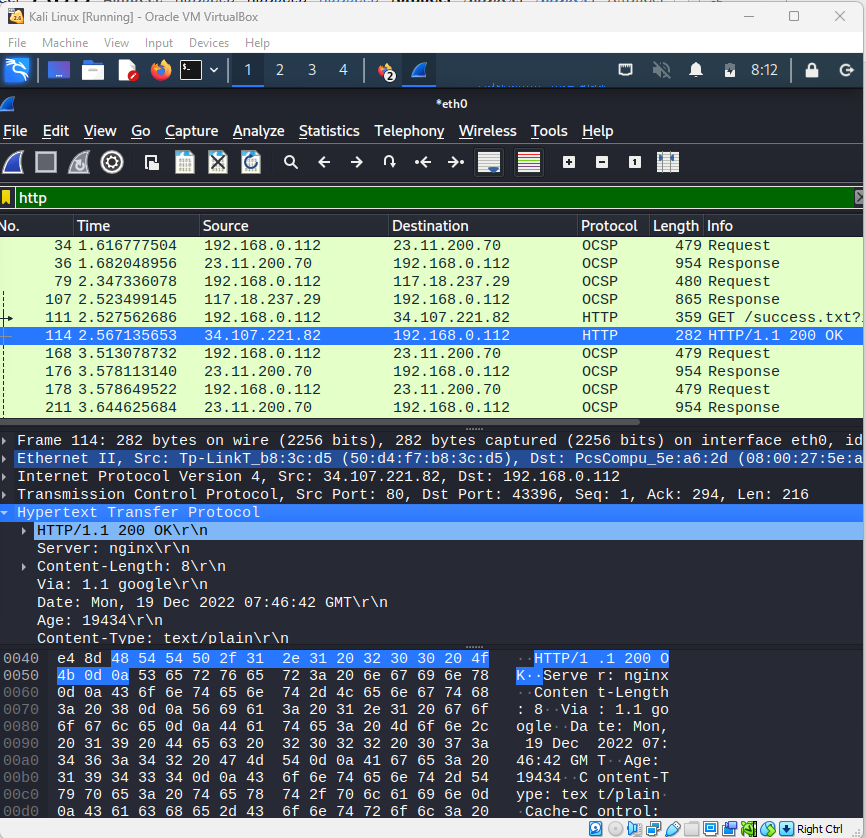
+ Chọn interface để bắt gói:



+ Bấm nút STOP



+ Ta có thể inspect một gói tin bằng cách click vào nó



* Đánh giá mức độ nguy hiểm của loại hình tấn công này:

+ Thu thập thông tin nhạy cảm

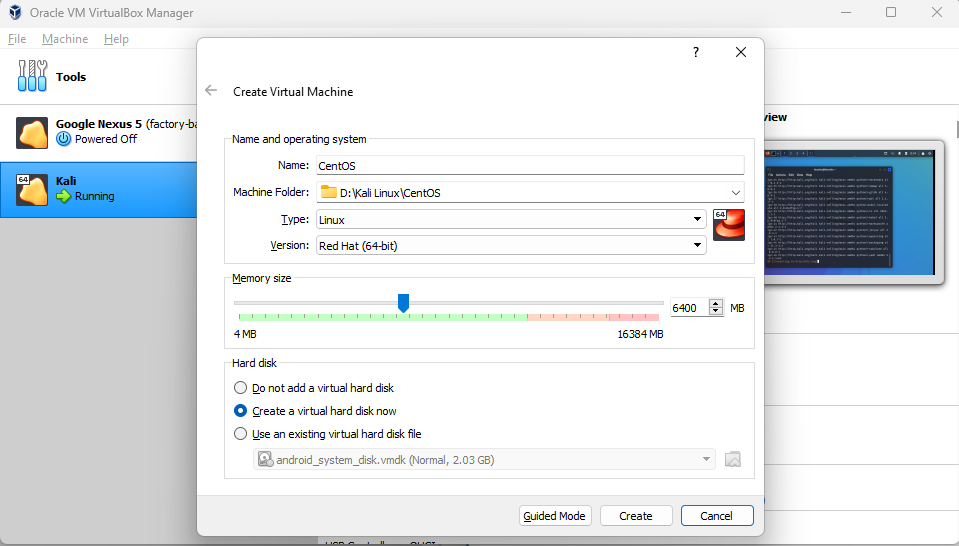
* Biện pháp đối phó đối với loại hình tấn công là gì ?

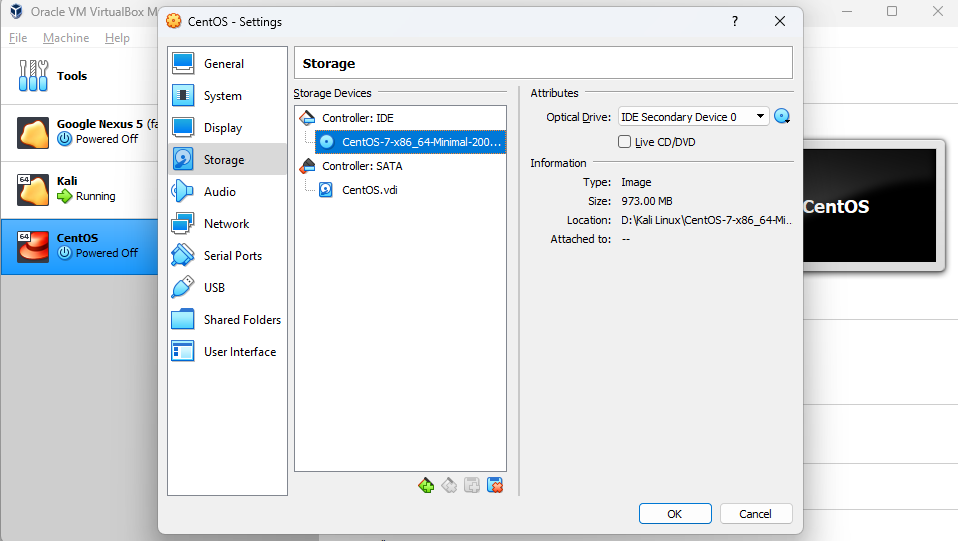
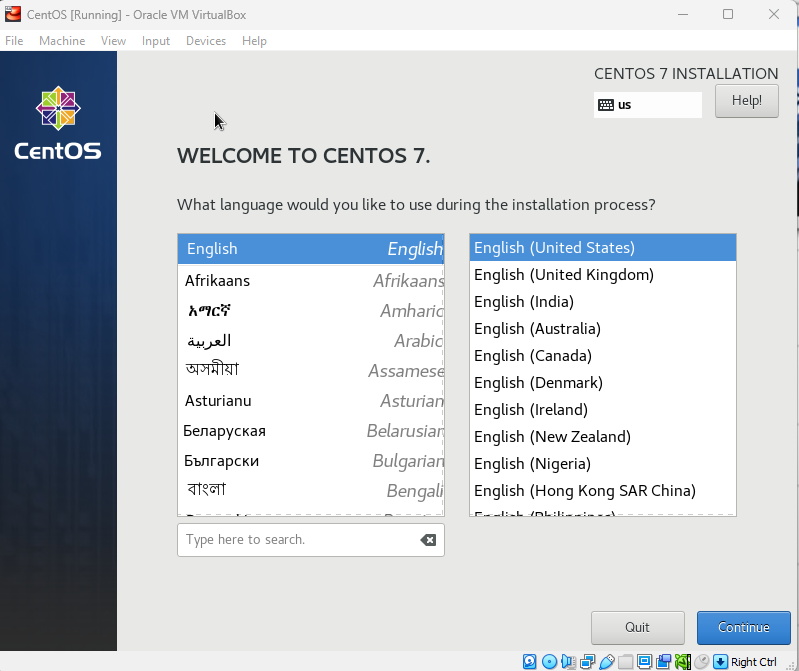
+ Các giao thức trên mạng: Mã hóa end – end -> Không thể bắt gói được

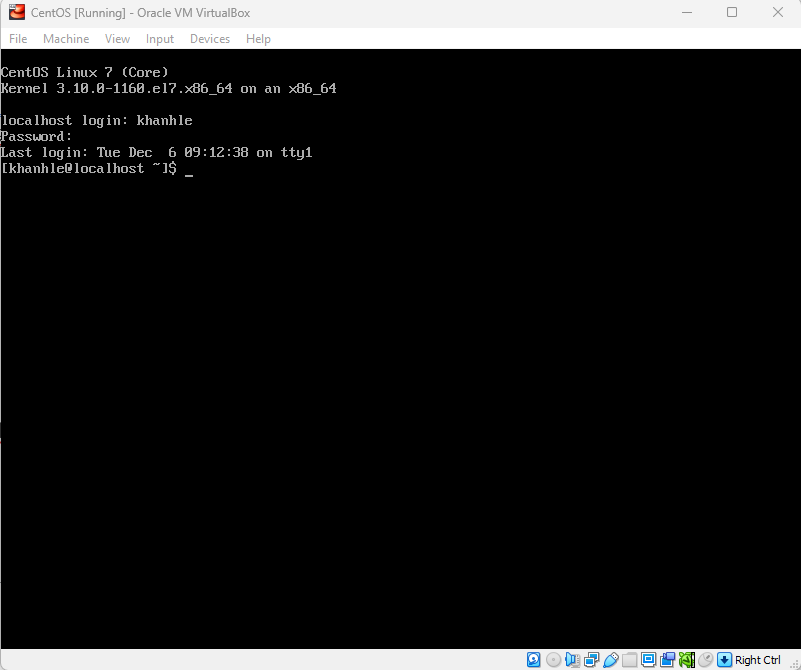
* + - * 1. **Cài đặt máy chủ CentOS 7**
* Hệ điều hành CentOS là gì ?

CentOS là một hệ điều hành miễn phí được xây dựng và phát triển dựa trên hệ điều hành mã nguồn mở Linux. CentOS là chữ viết tắt của “Community Enterprise Operating System”. CentOS ra mắt công chúng vào tháng 5 năm 2004 và được phát triển dựa trên bản phân phối của Red Hat Enterprise Linux (RHEL)

* Hãy cho biết các bước cài đặt máy chủ CentOS 7 trên Virtual Box bao gồm vài hình ảnh:

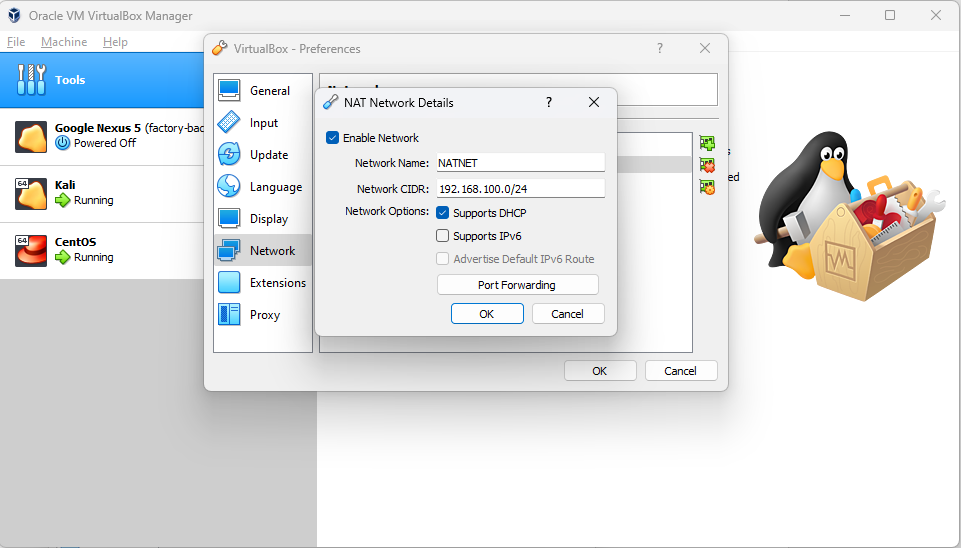


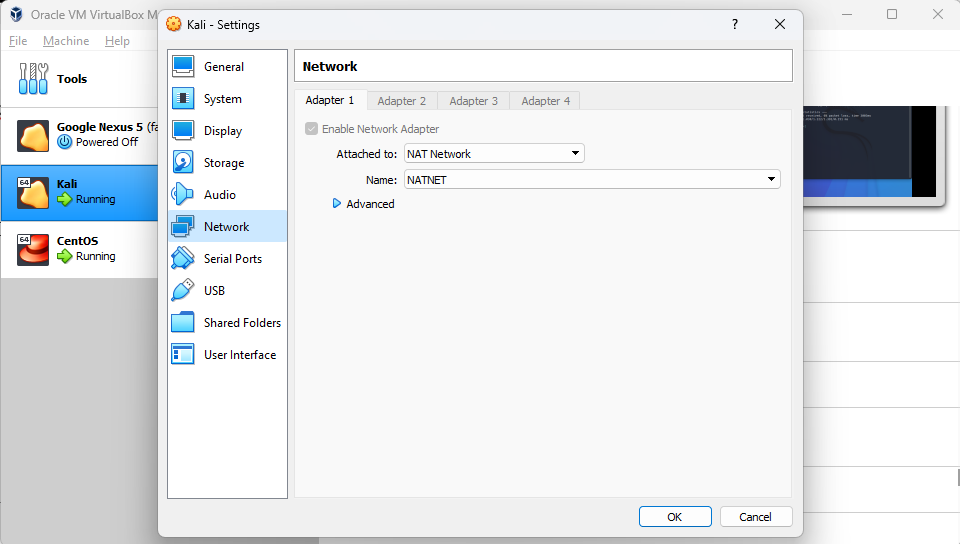


* Cấu hình để máy chủ CentOS và Kali Linux có thể ”thấy” nhau. Cho biết kết quả kiểm tra kết nối từ máy Kali linux đến máy chủ CentOS bằng lệnh ping:

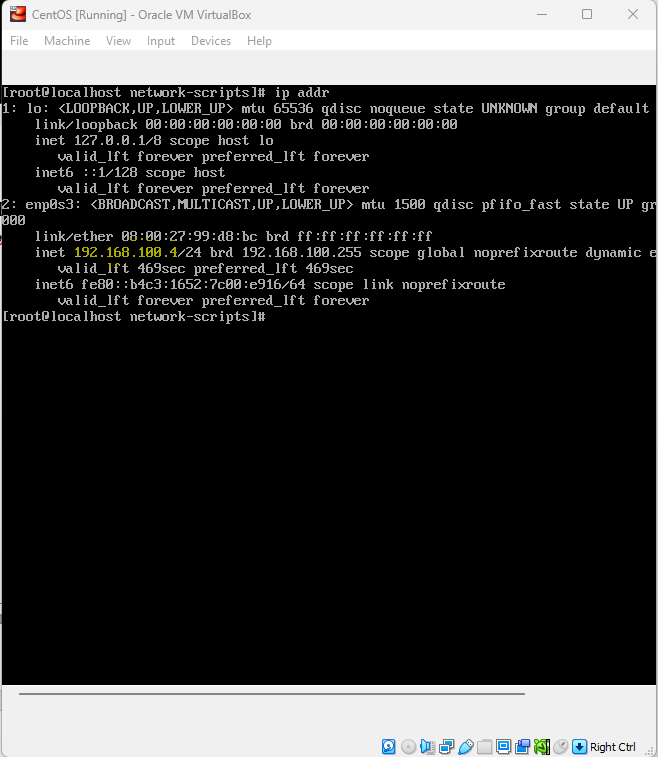
+ Từ VirtualBox chọn Tools -> Preferences -> NetWork rồi tạo NAT Network như bên dưới



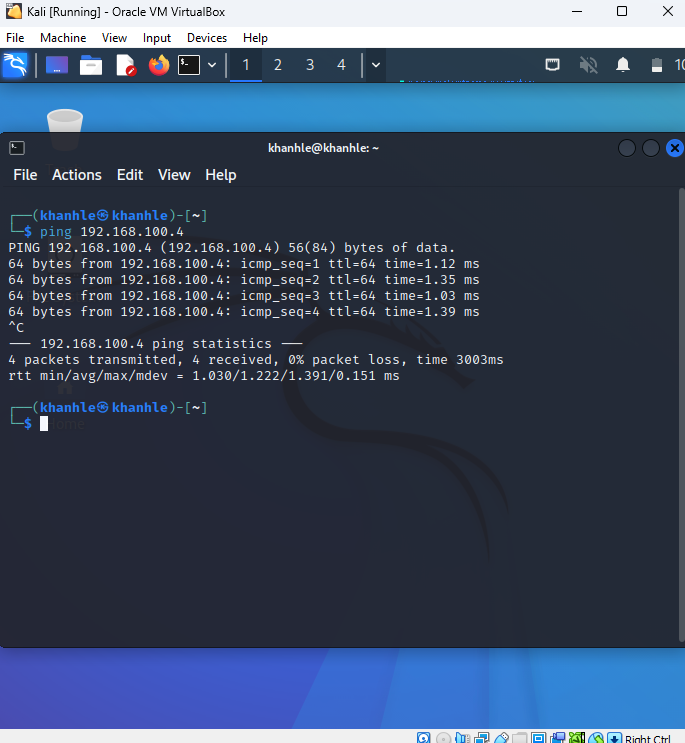
+ Setting NAT Network cho cả Kali Linux và CentOS

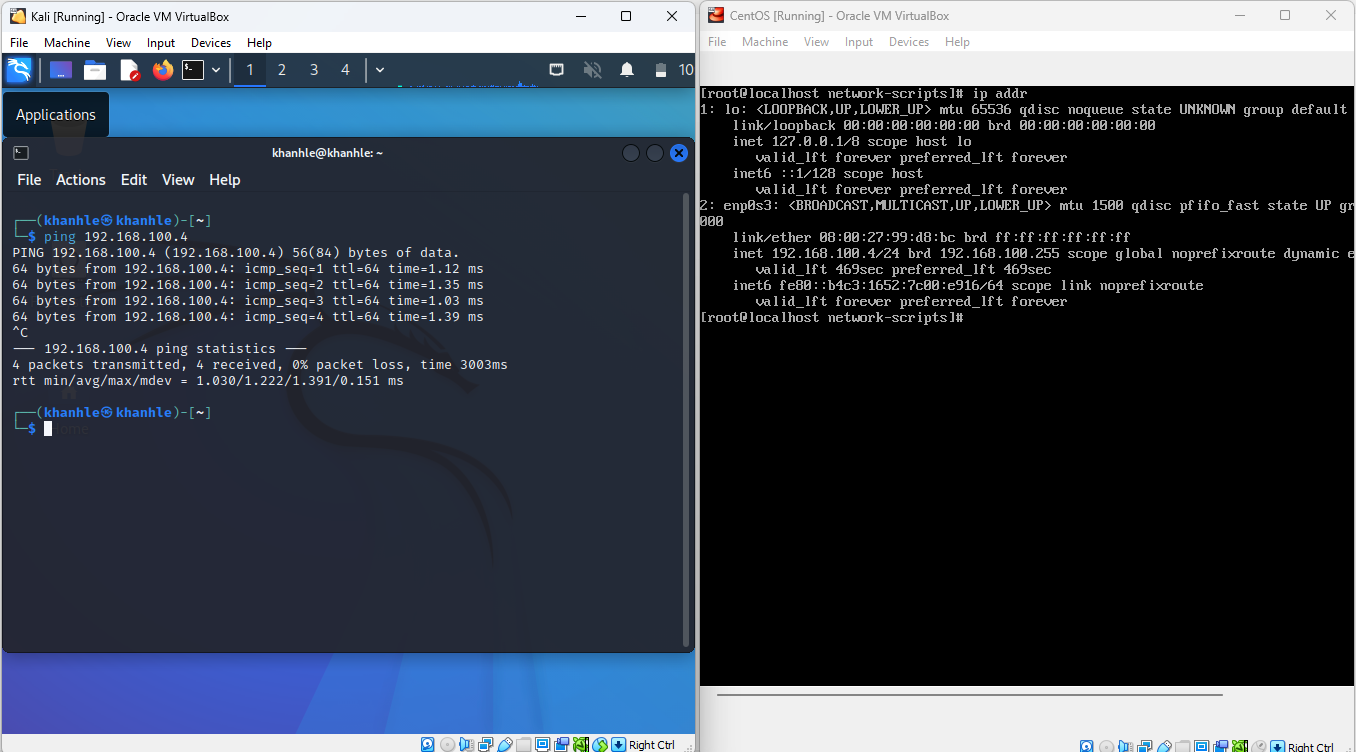


+ Địa chỉ IP của máy chủ CentOS: 192.168.100.4



+ Kết quả ping 192.168.100.4 từ máy Kali Linux





* + - * 1. **Tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7**
* Tìm hiểu và cho biết cách sử dụng công cụ hydra trên Kali Linux:

Hydra là một công cụ phổ biến để khởi động các cuộc tấn công vũ phu vào thông tin đăng nhập.

Hydra có các tùy chọn để tấn công thông tin đăng nhập trên nhiều giao thức khác nhau, nhưng trong trường hợp này, chúng ta sẽ tìm hiểu về cách kiểm tra độ mạnh của mật khẩu SSH. SSH có mặt trên bất kỳ máy chủ Linux hoặc Unix nào và thường là cách chính mà quản trị viên sử dụng để truy cập và quản lý hệ thống của họ.

Để bắt đầu, hãy chọn một máy trên cùng mạng để kiểm tra. Tìm địa chỉ IP của máy đó để ta có thể chỉ cho Hydra hướng tấn công. Khi đã có IP của máy mục tiêu, hãy mở terminal trong Kali. Dùng lệnh linux sau đây để kiểm tra mật khẩu SSH của người dùng root.

$ hydra -l root -p admin 192.168.100.4 -t 4 ssh

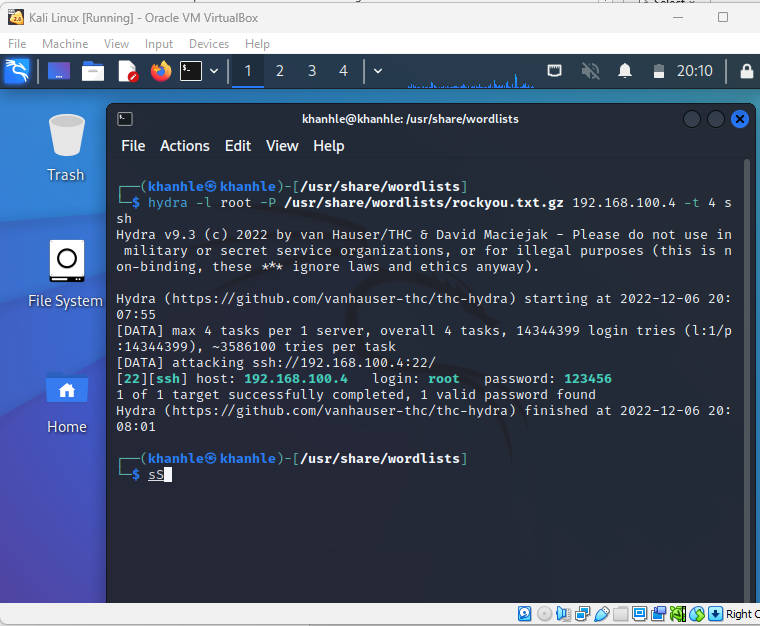
Với -l flag sử dụng một user parameter, -p flag sử dụng một password, địa chỉ IP là địa chỉ IP của máy bị tấn công, -t là số threads sử dụng, ssh tức là Hydra sẽ tấn công SSH

Reference: <https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux>

* Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 với tự điển hiện có:

$ hydra -l root -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.4 -t 4 ssh

+ Kết quả

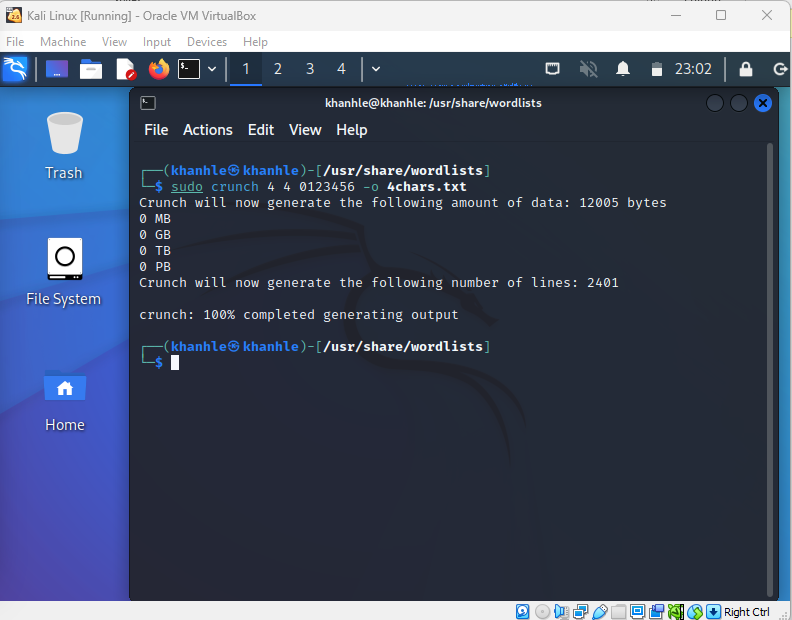


+ Kết quả ta thu được password 123456 ứng với user root

* Tạo danh sách các mật khầu (wordlist) bằng crunch và dùng hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 dùng danh sách mật khẩu đã tạo ra:

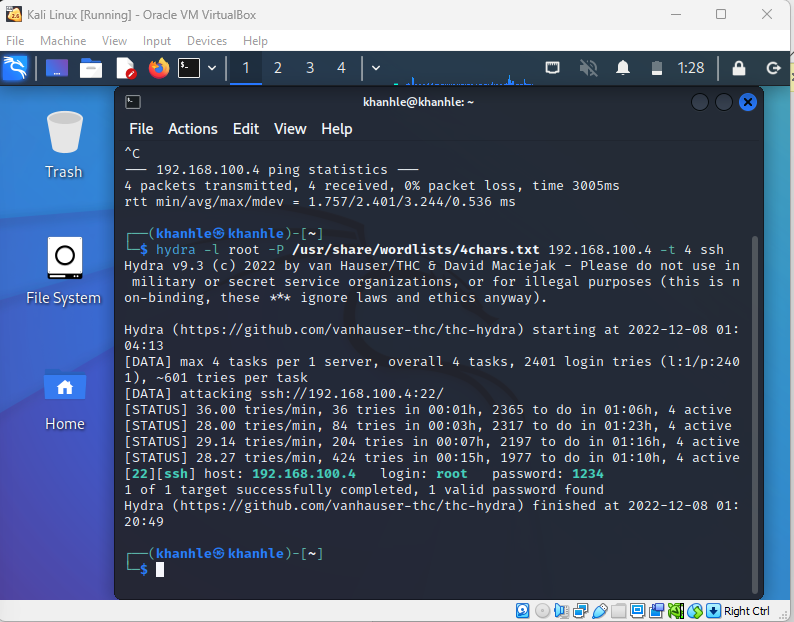
+ Tạo danh sách các mật khầu (wordlist)

$ sudo crunch 4 4 0123456 -o 4chars.txt



+ Thử chạy lại với wordlist mới

$ hydra -l root -P /usr/share/wordlists/4chars.txt 192.168.100.4 -t 4 ssh



* Đánh giá mức độ nguy hiểm của loại hình tấn công này:

+ Mức độ nguy hiểm lớn

+ Có thể mất thời gian nhưng nếu có được mật khẩu của người quản trị thì có thể sử dụng để chiếm quyền admin

* + - * 1. **Giải pháp giảm thiểu tấn công vét cạn**
* Tìm hiểu fail2ban và cho biết nó được sử dụng để làm gì ?

Fail2ban là 1 chương trình được viết bằng python có nhiệm vụ chặn các ip kết nối đến server dựa vào các dấu hiệu nghi ngờ mà ip đó để lại trong file log của hệ thống hoặc dịch vụ. Ví dụ như có quá nhiều lần sử dụng mật khẩu không hợp lệ, truy cập không hợp lệ hoặc các dấu hiệu bất thường khác mà có thể nhận biết được. Ta có thể cài đặt Fail2ban trên Centos 7 cấu hình chống bruteforce attack cho SSH và WordPress.

Reference:

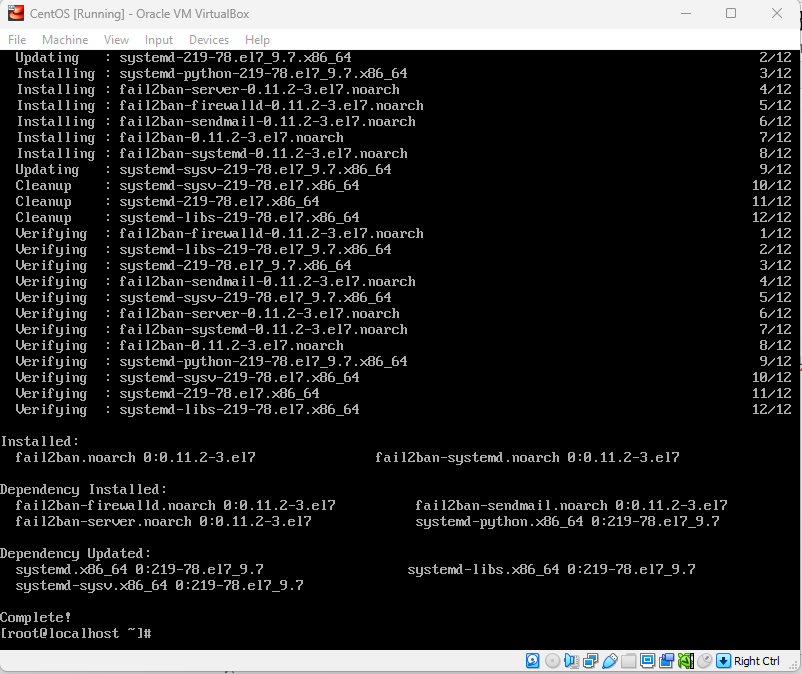
<https://blog.hostvn.net/chia-se/cai-dat-fail2ban-tren-centos-7-chong-bruteforce-attack.html>

* Cài đặt và cấu hình fail2ban đối với dịch vụ SSH trên máy chủ CentOS 7:

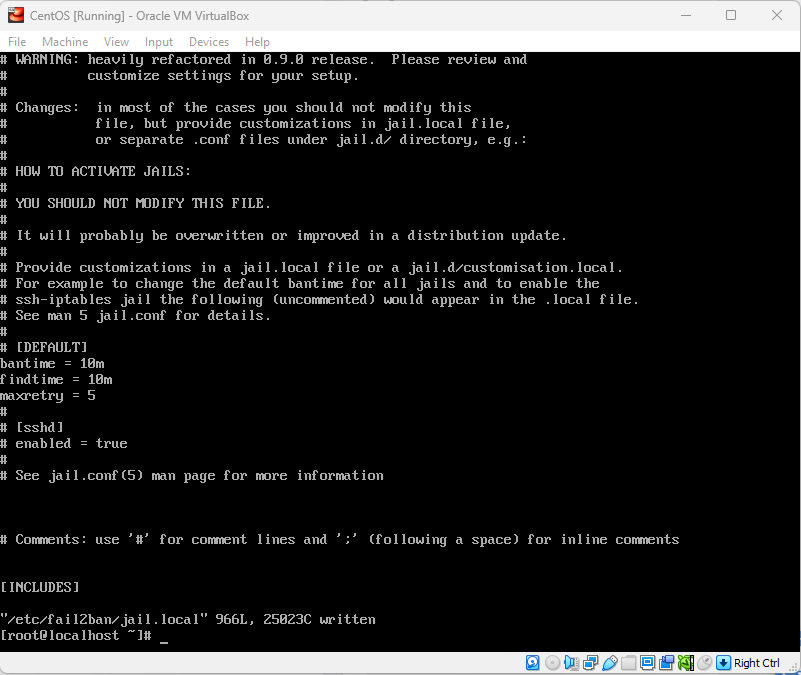
+ Cài đặt Fail2Ban trên CentOS 7

$ yum -y install epel-release

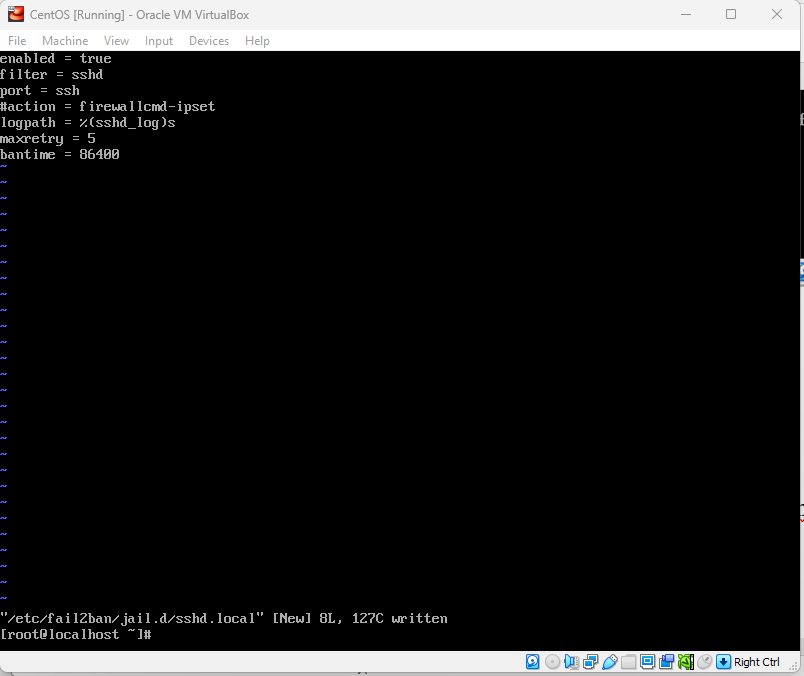
$ yum -y install fail2ban fail2ban-systemd



+ Cấu hình Fail2Ban



+ Bảo vệ SSH



+ Khởi động Fail2ban:

