Đỗ Trần Nhật Tân

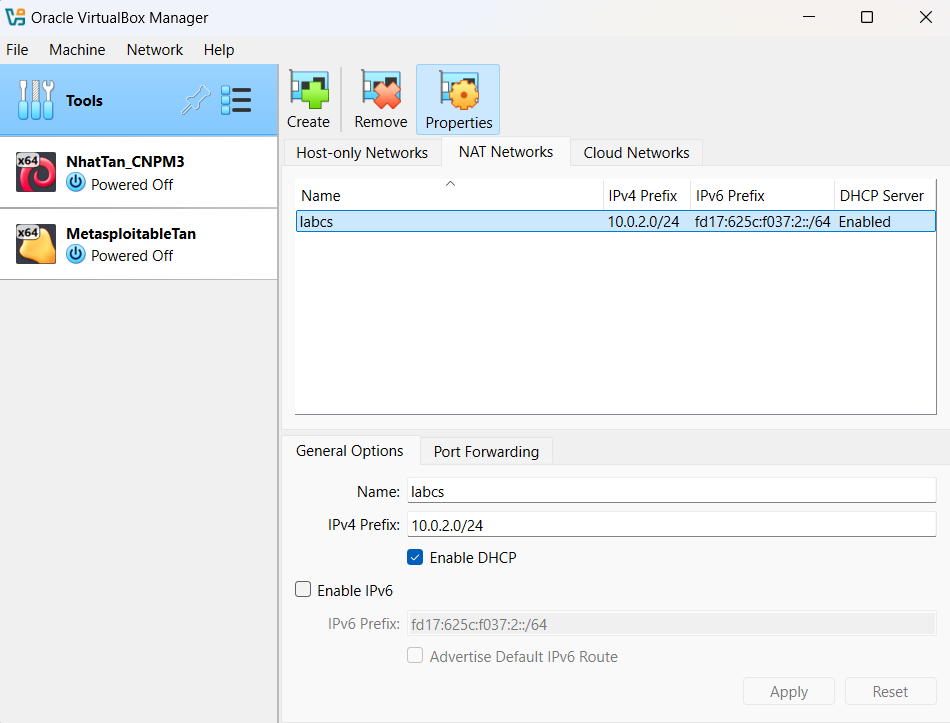
1050080198

10ĐH\_CNPM3

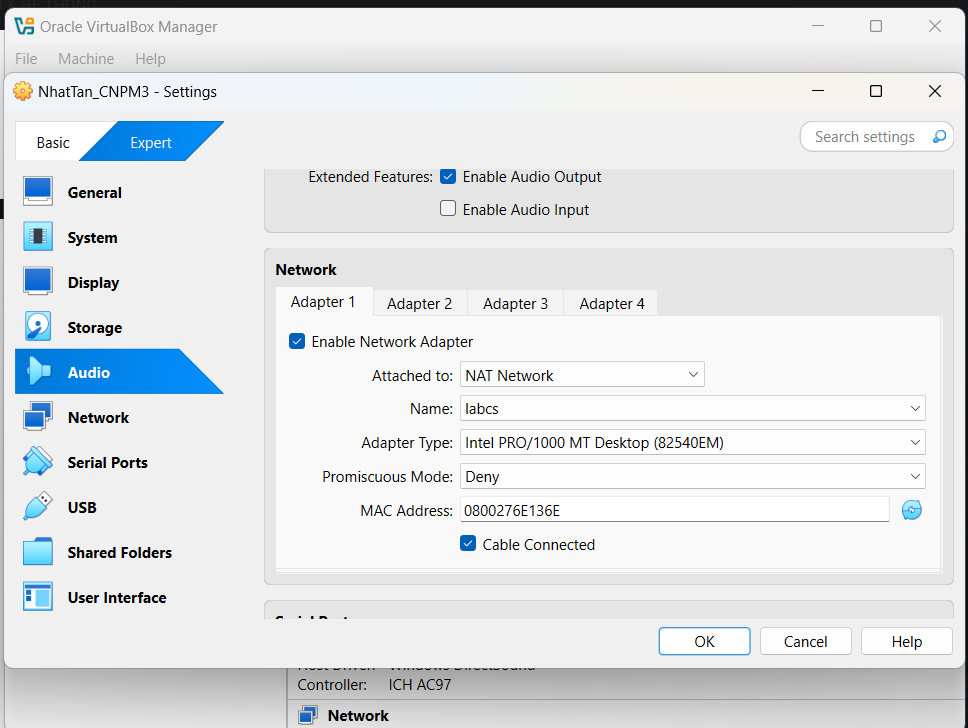
Lab 1 an ninh mạng

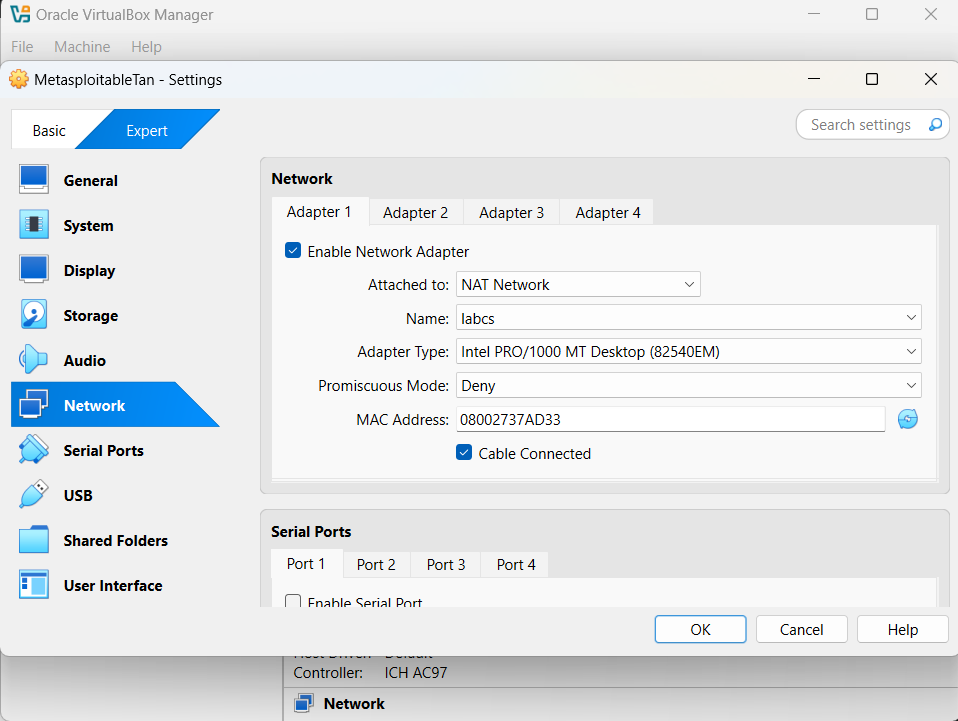
Câu 1:

1. Tạo nat network tên labcs

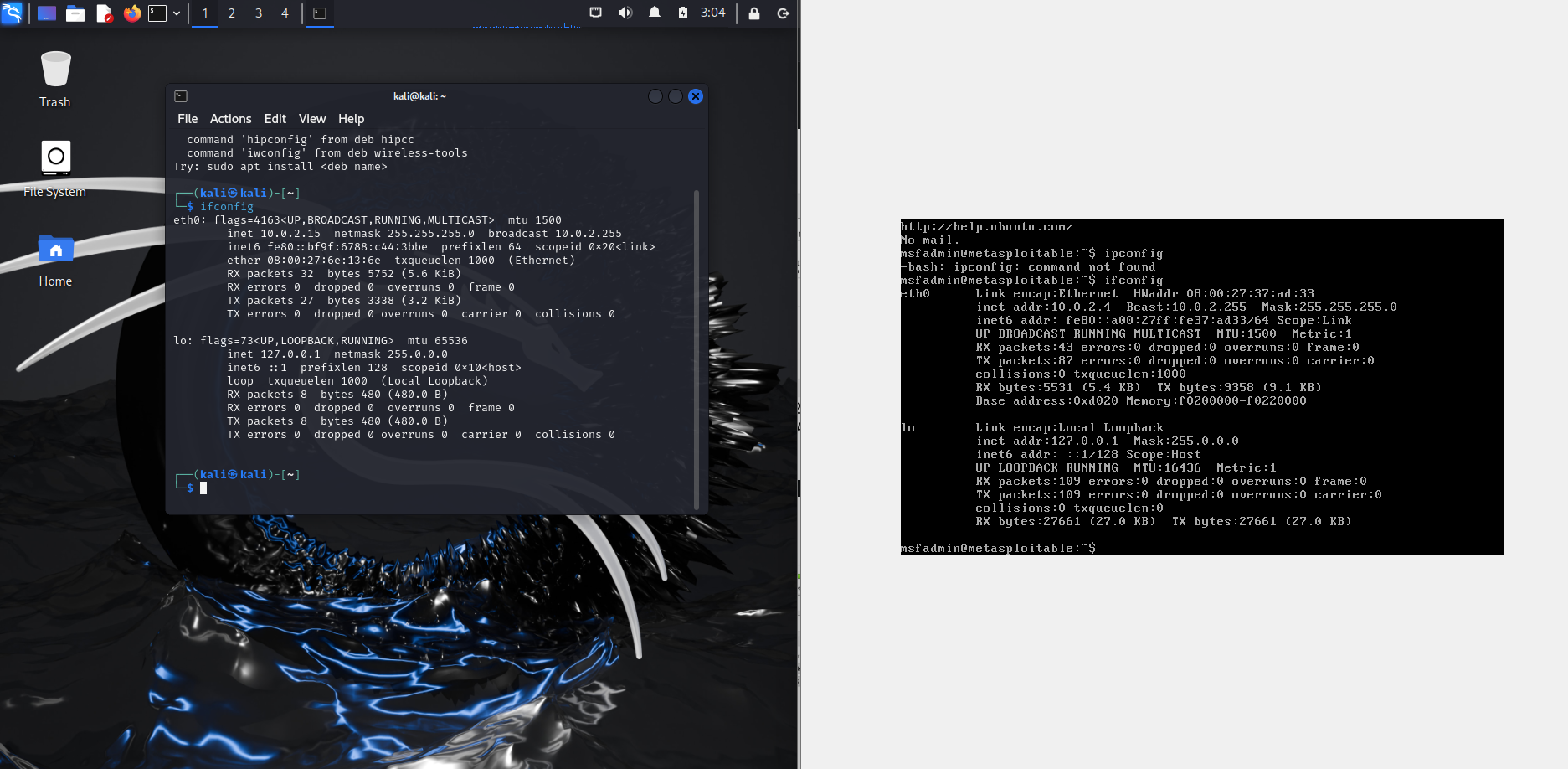


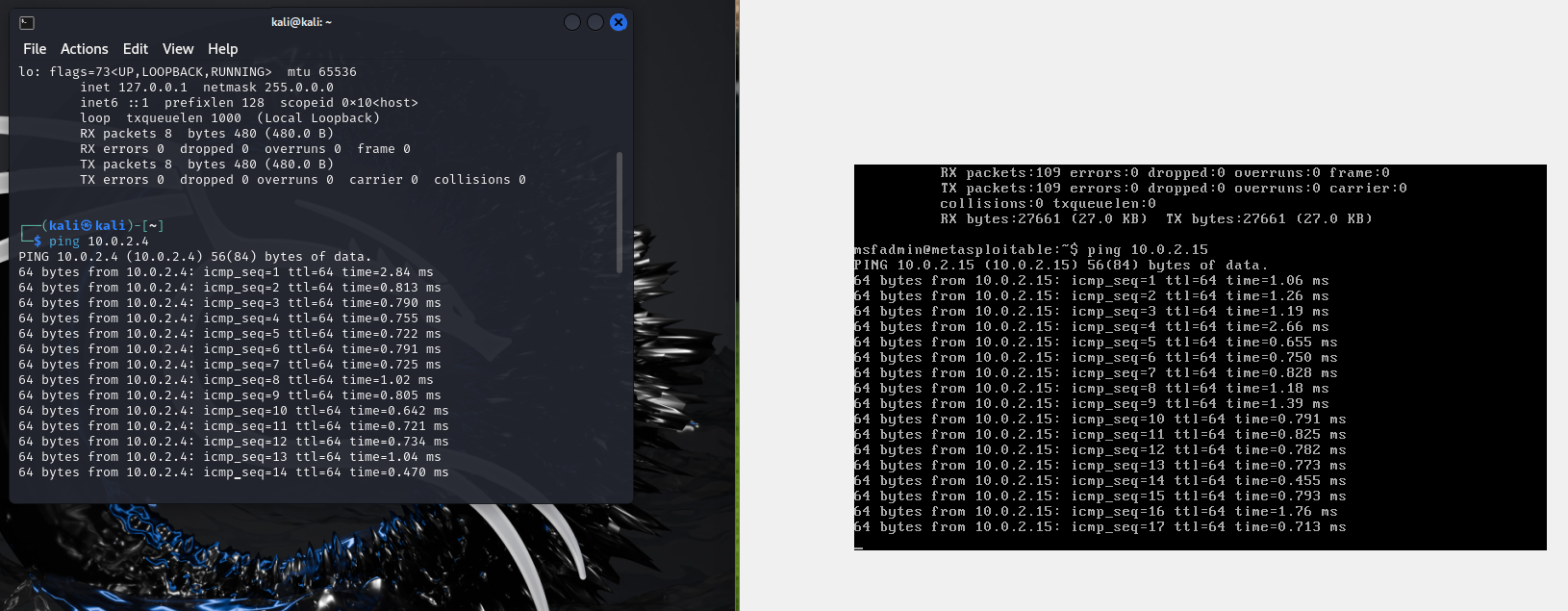
1. Tạo 2 máy ảo và cấu hình cho 2 máy ảo mạng NAT





1. Kiểm tra IP 2 máy ảo



1. Ping kiểm tra kết nối  
   

Máy kali IP là 10.0.2.15

Máy Meta IP là 10.0.2.4

Câu 2:

2.1

Trả lời câu hỏi:

+Chức năng chính của Nmap là gì?

Trên Kali Linux, Nmap (“Network Mapper”) chủ yếu được sử dụng để:

Phát hiện host: Xác định các máy chủ hoặc thiết bị đang hoạt động trong mạng (Host Discovery).

Quét cổng: Kiểm tra và liệt kê các cổng mở, đóng hay bị lọc trên từng host.

Xác định dịch vụ và phiên bản: Phân tích các dịch vụ (service) đang chạy trên các cổng mở, bao gồm tên, phiên bản và thông tin liên quan.

Phân tích hệ điều hành (OS Fingerprinting): Dựa trên các phản hồi của gói tin, Nmap có thể đoán được hệ điều hành của máy chủ mục tiêu.

Sử dụng Nmap Scripting Engine (NSE): Cho phép chạy các script để tự động phát hiện lỗ hổng, kiểm tra cấu hình bảo mật hoặc thu thập thông tin chuyên sâu.

Nhờ vào những chức năng này, trên Kali Linux – một bản phân phối chuyên về bảo mật – Nmap trở thành công cụ không thể thiếu cho quá trình trinh sát và đánh giá bảo mật hệ thống.

+Liệt kê một số tham số trọng của Nmap.

Một số tham số quan trọng của Nmap bao gồm:

-sS: Thực hiện TCP SYN scan (còn gọi là “half-open scan” hay stealth scan), giúp quét nhanh và khó bị phát hiện.

-sT: TCP connect scan – sử dụng khi không có quyền root (sử dụng API của hệ điều hành để thiết lập kết nối TCP đầy đủ).

-sU: UDP scan – quét các cổng UDP để xác định trạng thái (open|filtered, closed, …).

-p: Chỉ định các cổng cần quét, ví dụ: -p 22,80,443 hoặc quét dãy cổng -p 1-65535.

-sV: Phát hiện phiên bản của dịch vụ đang chạy trên các cổng mở.

-O: Phát hiện hệ điều hành (OS fingerprinting) của máy chủ mục tiêu.

-A: Quét toàn diện – kết hợp OS detection, version detection, script scanning và traceroute.

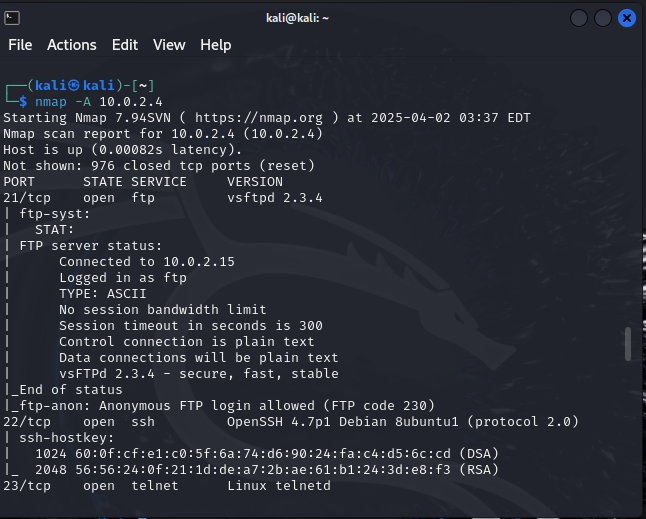
-Pn: Bỏ qua bước host discovery (giả sử host luôn online) để tiết kiệm thời gian.

-v: Verbose – tăng mức độ chi tiết trong đầu ra.

--script: Cho phép chạy các script từ Nmap Scripting Engine (NSE) để mở rộng chức năng, ví dụ --script=http-title.

2.2

Nmap -A 10.0.2.4





2.3

Dịch vụ trên cổng 21 là vsftpd 2.3.4.

Gồm những lỗ hổng bảo mật:

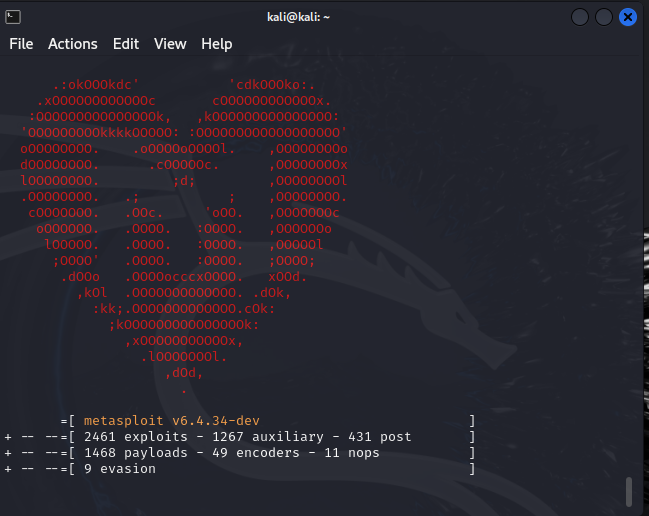
Backdoor Trigger: Nếu một kết nối đăng nhập sử dụng tên người dùng kết thúc bằng ký tự “:)”, phần mềm sẽ kích hoạt một backdoor.

Hậu quả: Backdoor này mở một shell từ xa (thường là trên cổng 6200), cho phép kẻ tấn công thực thi các lệnh trên hệ thống mà không cần xác thực thêm.

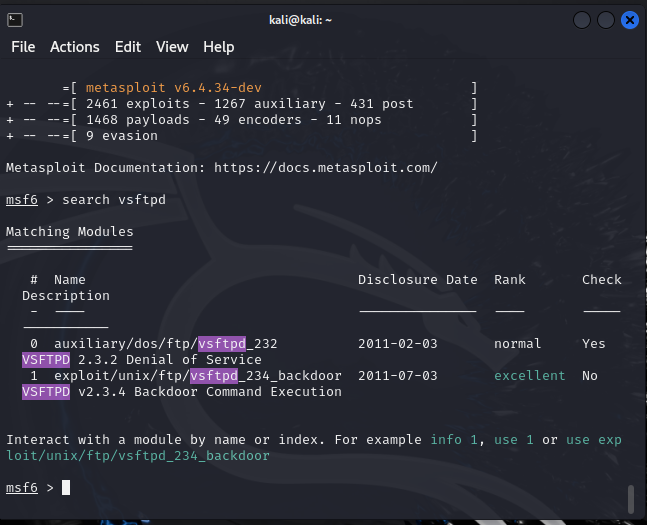
Lưu ý chung: Ngoài lỗ hổng backdoor, FTP nói chung cũng truyền dữ liệu (bao gồm cả mật khẩu) ở dạng không mã hóa, tạo điều kiện cho việc nghe lén.

2.4

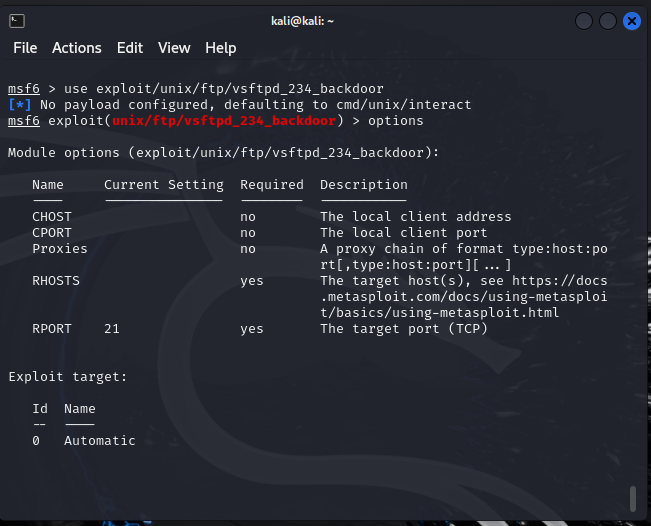
Chạy lệnh msfconsole



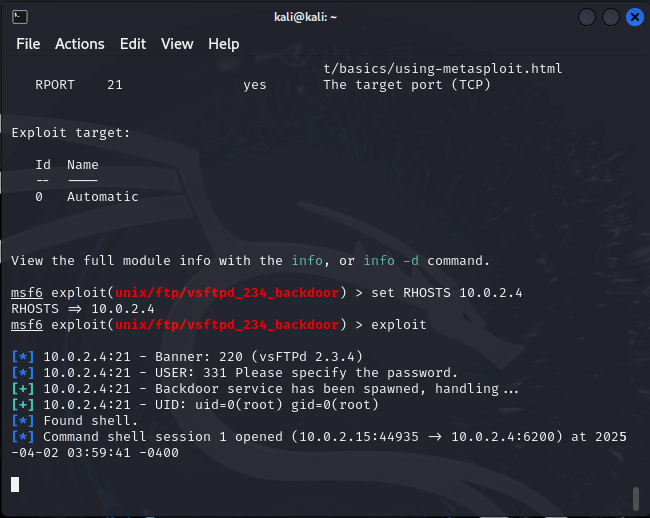
Search vsftpd



Dùng lệnh search vsftpd để khai thác lỗ hổng bảo mật, sau đó dùng lệnh use để sử dụng công cụ và dùng lệnh options để xem tham số.



Dùng exploit để khai thác

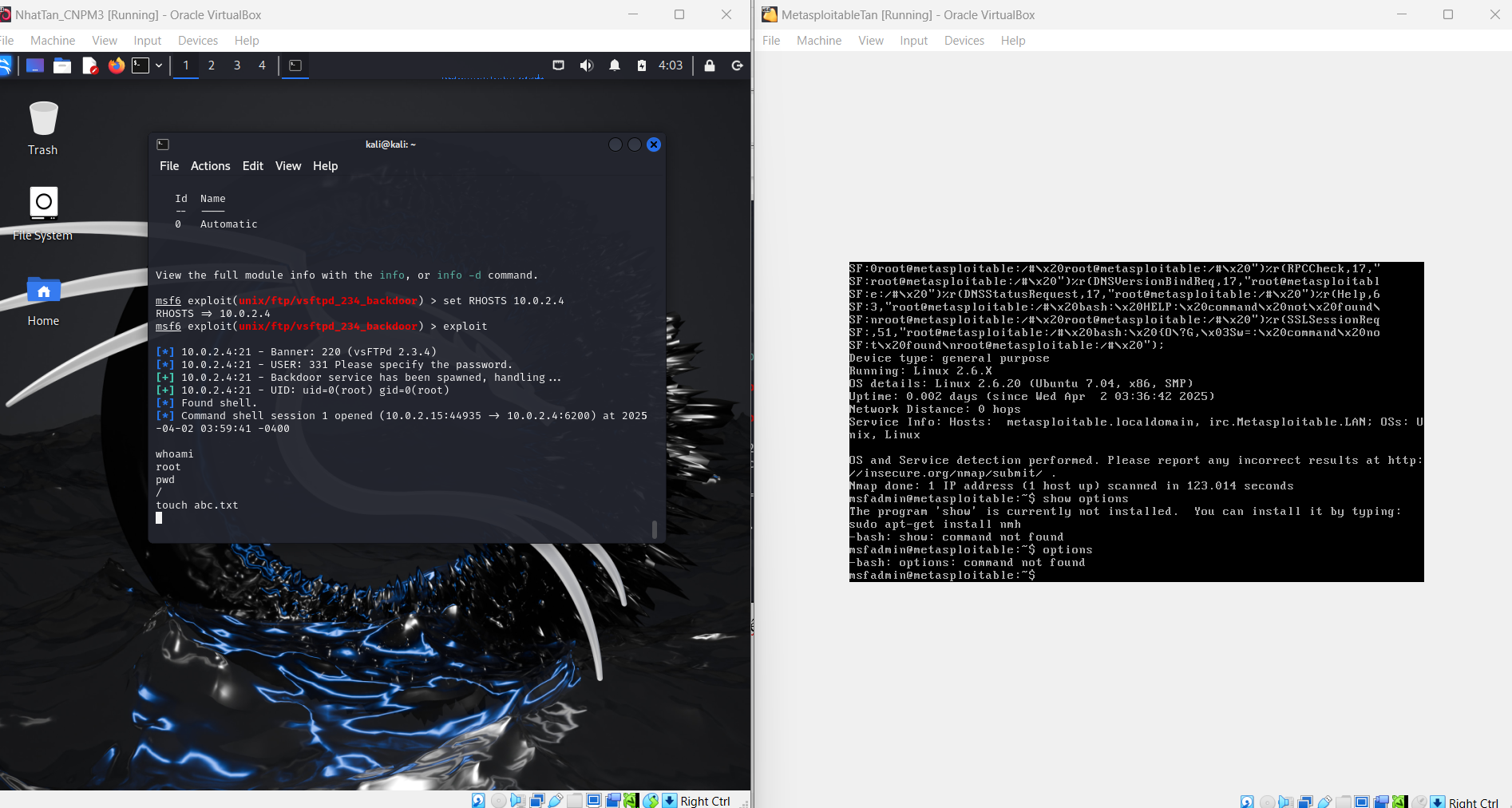


Ta gõ các lệnh để thực hiện trên máy mục tiêu

Whoami

Pwd

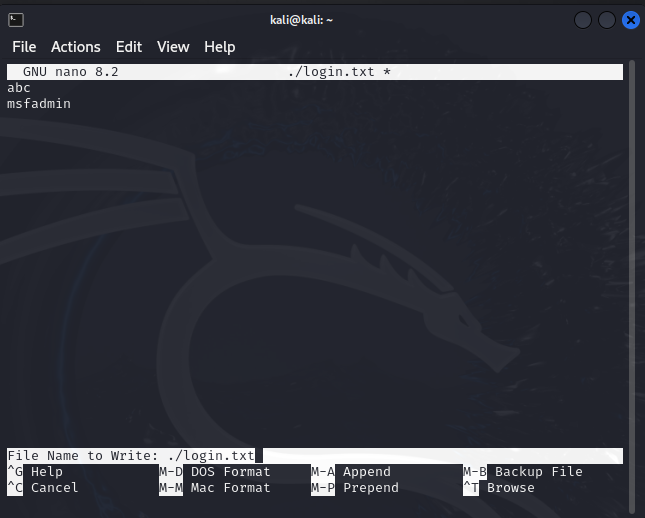
Touch abc.txt



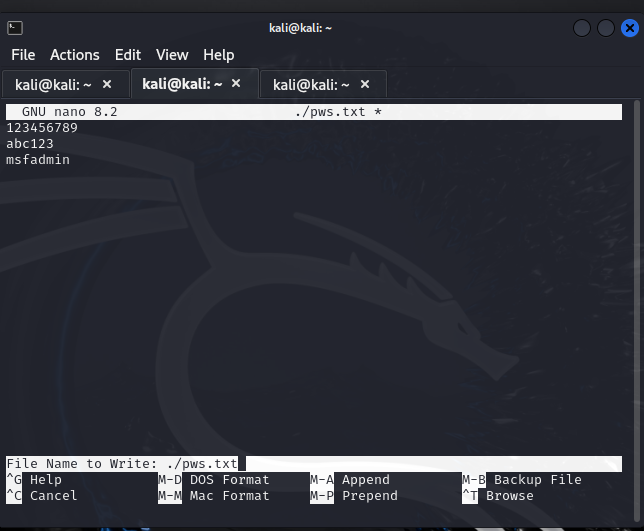
2.5

Tạo 2 file login.txt là pws.txt

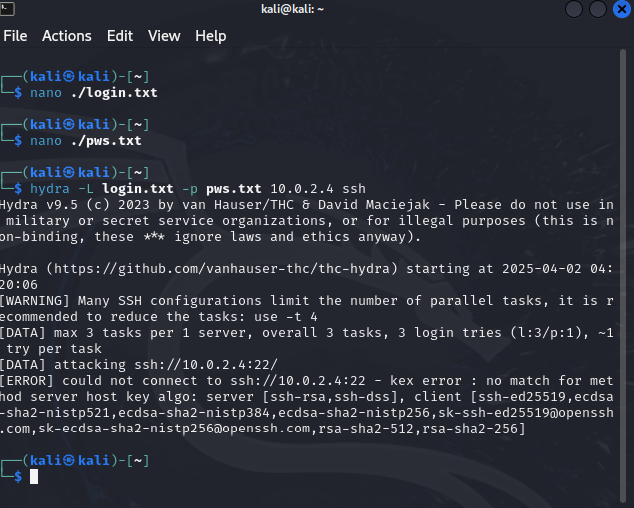
Login.txt



Pws.txt

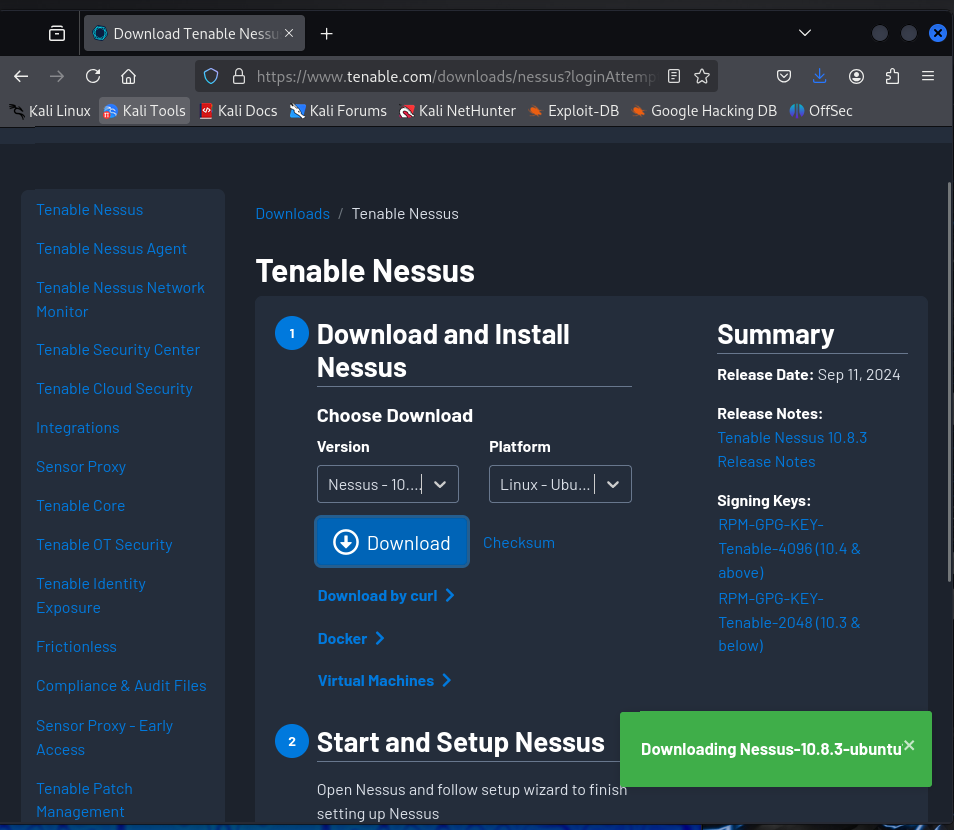


dùng lệnh hydra –L logins.txt –P pws.txt 10.0.2.4 ssh để tấn công và tìm mật khẩu

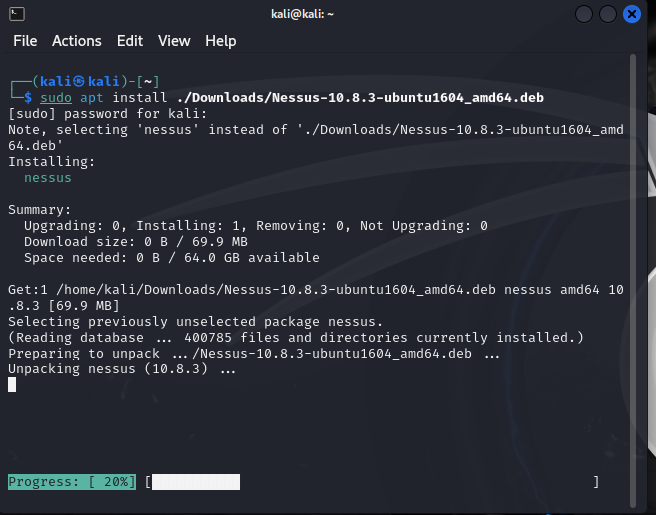


Cách 3

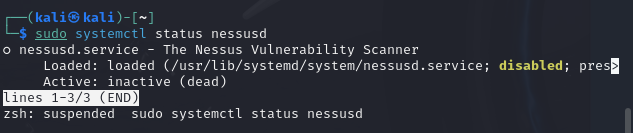
Download tenable nessus



Cài đặt Nessus

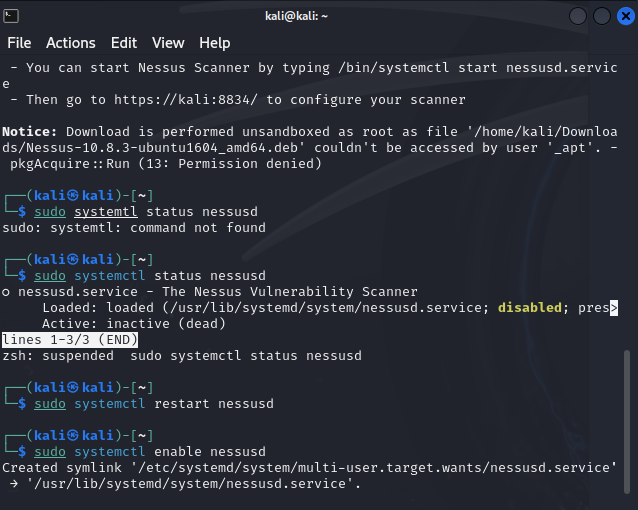


Dùng lệnh sudo systemctl status nessusd để kiểm tra trạng thái



Khởi động lại nessus

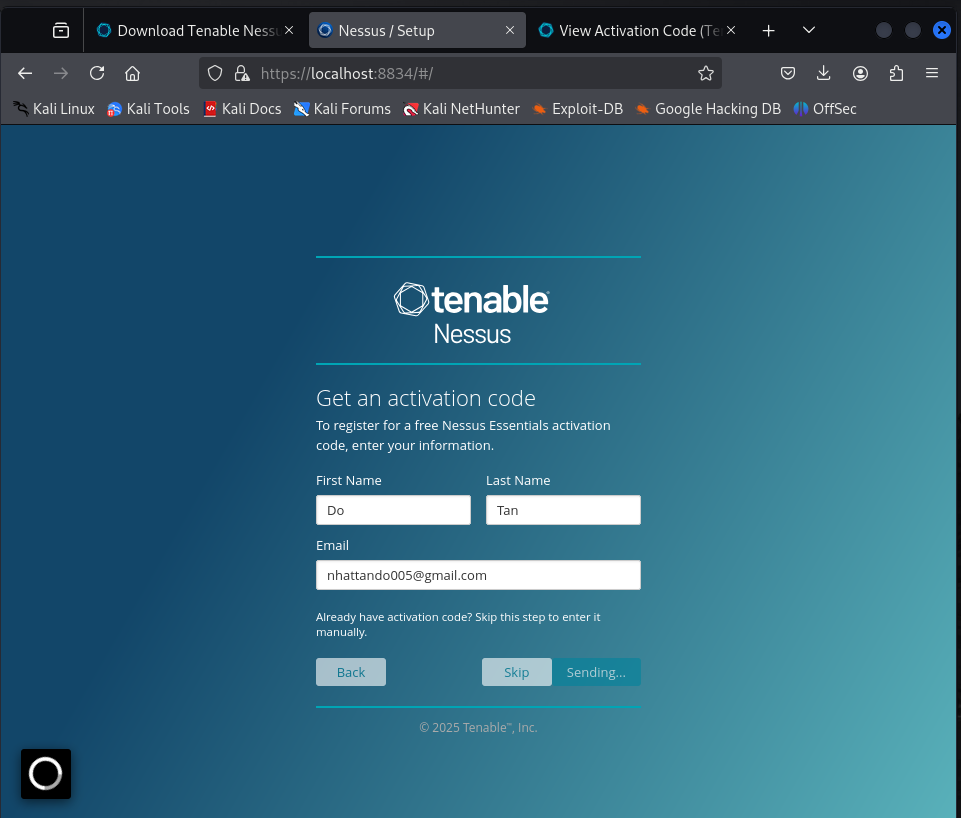
Sudo systemctl restart nessusd



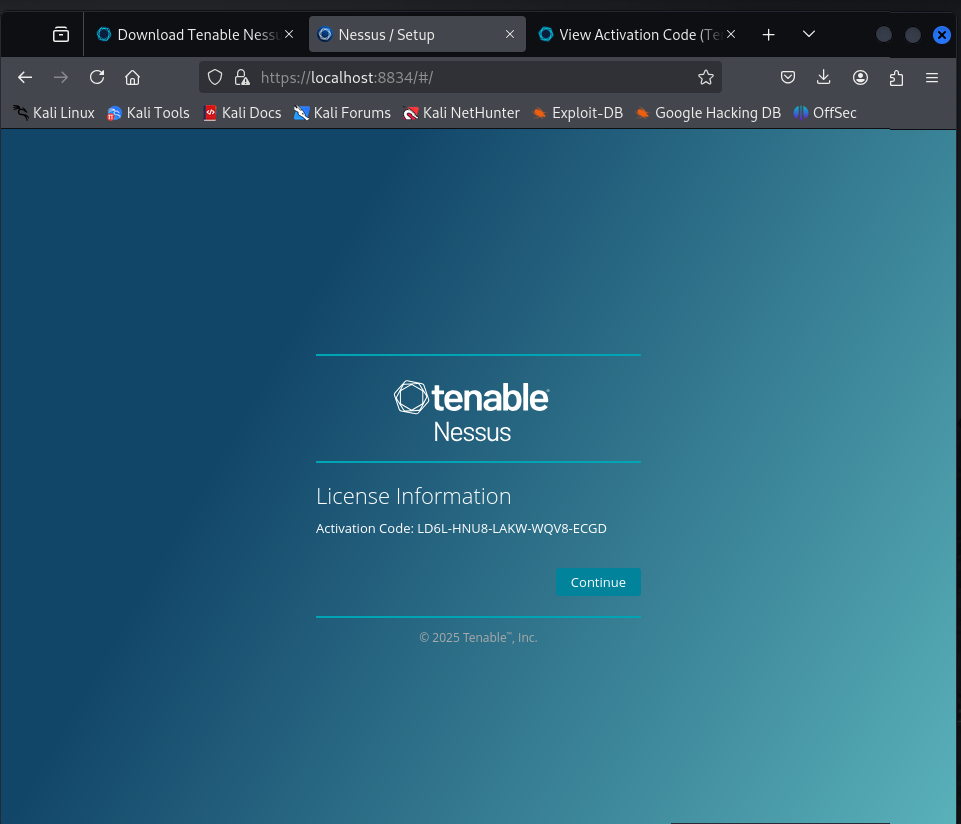
Sau khi khởi động lại nessus, truy cập <https://localhost:8834> để đăng kí activation code

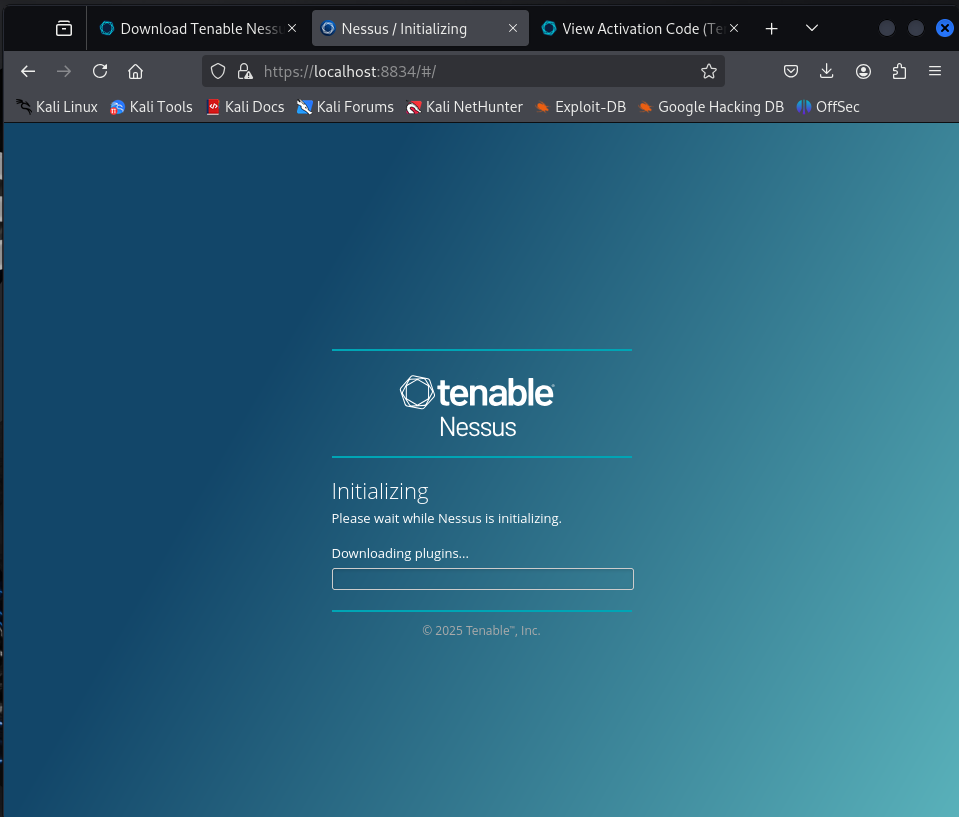


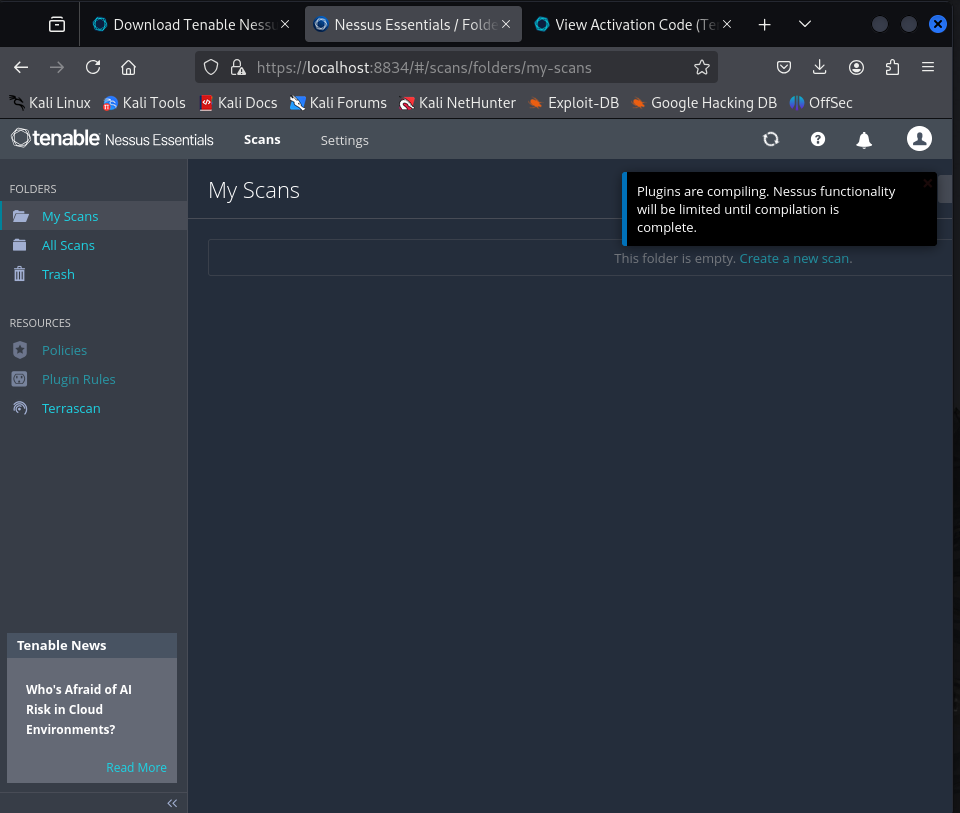
Diền thông tin



Nhận activation code



Download plugin  




Bài 4

Truy cập <https://www.offensive-security.com/labs/individual/> để tạo tài khoản