Lưu Thy Thy

1050080078

10ĐH\_CNPM1

Bước 1: Download phần mềm Virtualbox tại địa chỉ sau và cài đặt như một phần mềm thông thường trên Windows:

https://download.virtualbox.org/virtualbox/6.1.12/VirtualBox-6.1.12-139181-Win.exe

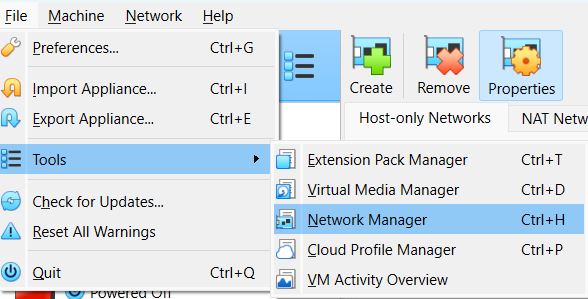
Bước 2: Download gói mở rộng cho Virtualbox từ địa chỉ sau:

https://download.virtualbox.org/virtualbox/6.1.12/Oracle\_VM\_VirtualBox\_Extension\_Pack-6.1.12.vbox-extpack

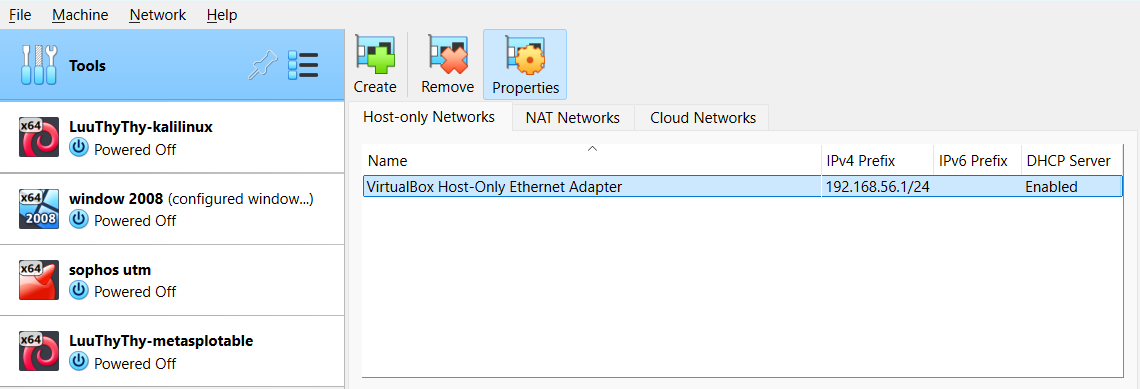
Sau khi download xong, nhấp đúp chuột vào file để cài đặt.

Bước 3: Khởi động phần mềm Virtualbox

Bước 4: Trên giao diện của Virtualbox, chọn File → Host Network Manager...

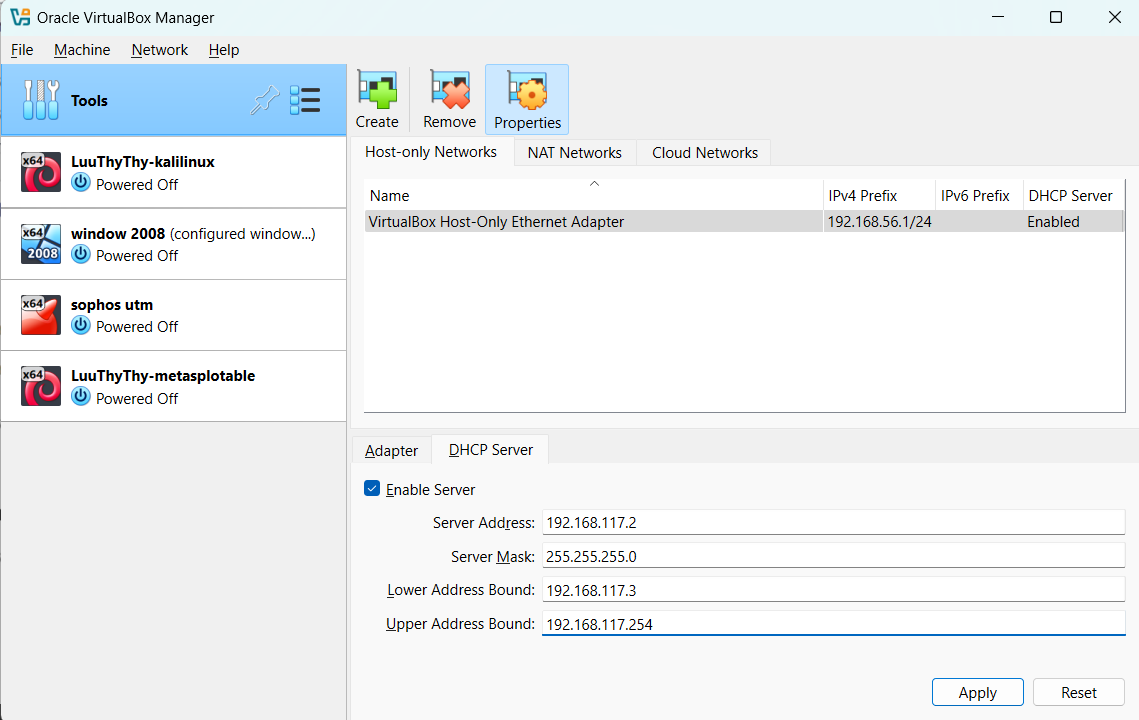


Bước 5: Chọn cạc mạng ảo VirtualBox Host-Only Ethernet Adapter. Chọn



Bước 6: Chọn thẻ Adapter và lựa chọn Configure Adapter Automatically.

Bước 7: Chọn thẻ DHCP Server và thiết lập các thông số như hình ảnh sau:

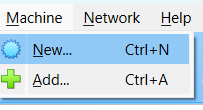


Bước 8: Nhấp nút Apply và Close để hoàn tất.

Bước 9: Download máy ảo từ địa chỉ sau và giải nén

<https://drive.google.com/file/d/1LSK_CZoha8LIKqr-8KkfyztZ6MM> eEF2/view?usp=sharing

Bước 10: Trên cửa sổ chính của Virtualbox, chọn Machine → New...



Bước 11: Trên cửa sổ tạo máy ảo, đặt các thông số như sau. Sau đó nhấn Next.

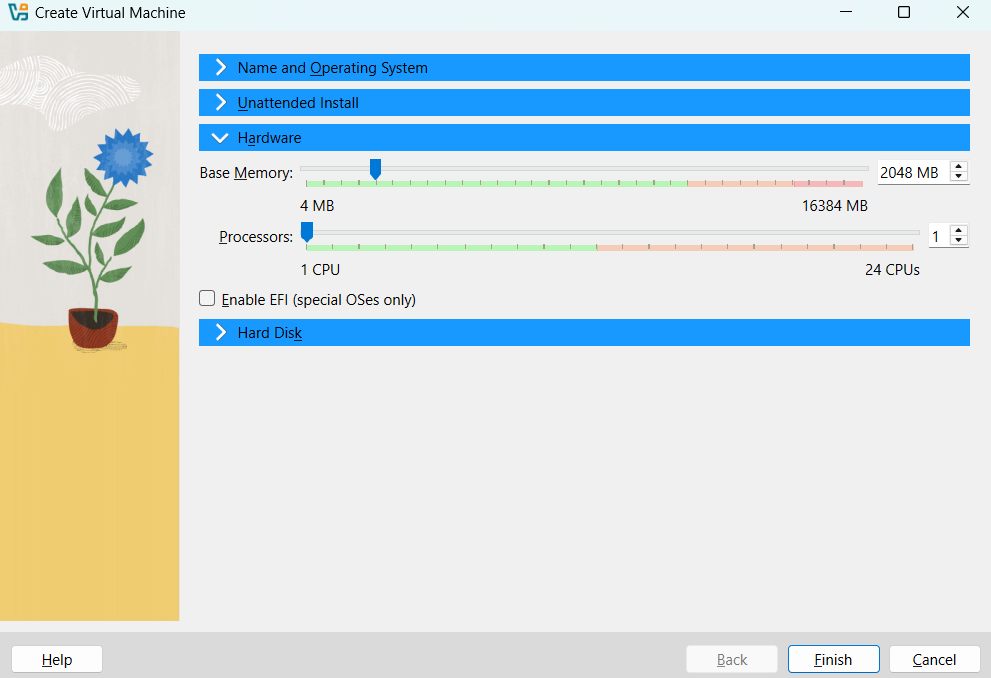
➢ Name: Tên máy ảo

➢ Machine Folder: Thư mục chứa máy ảo

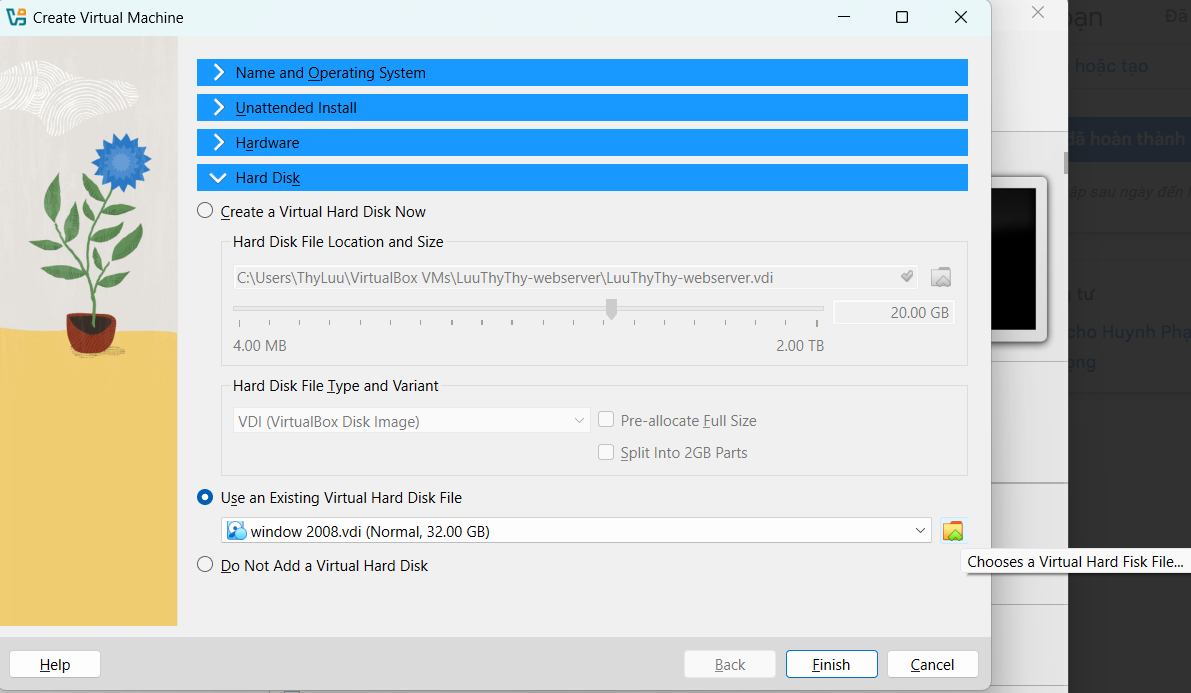
➢ Type: Linux

➢ Version: Ubuntu (32-bit)

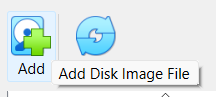
Bước 12 : Chọn dung lượng bộ nhớ RAM cho máy ảo là 2048 MB. Nhấn Next để tiếp tục.

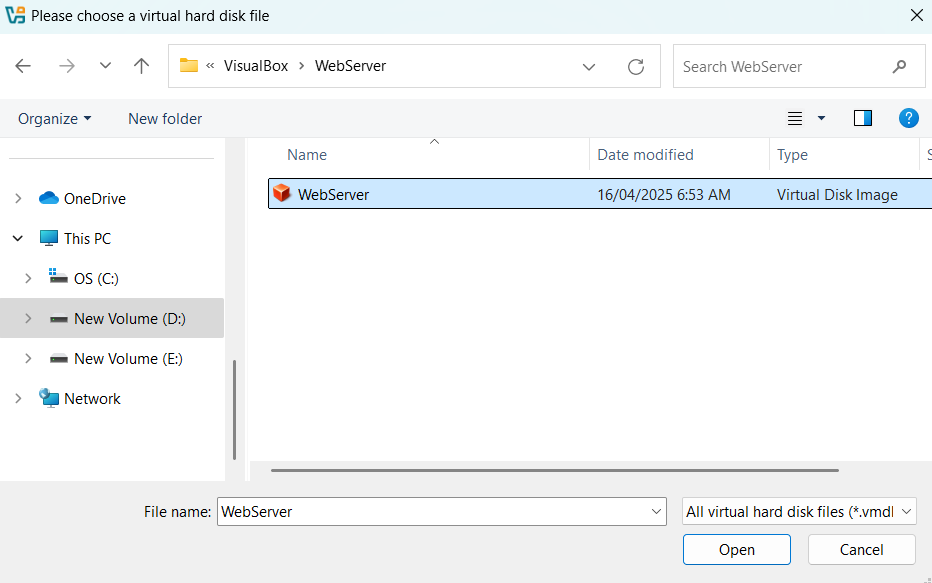


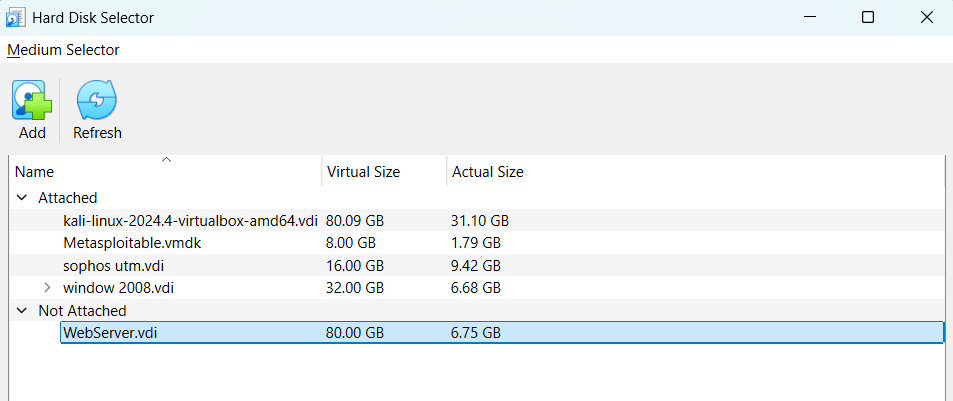
Bước 13 : Trong cửa sổ Hard disk tạo ổ cứng máy ảo, chọn mục Use an existing virtual hard disk file. Sau đó bấm nút Choose a virtual hard disk file...



Bước 14: Trên cửa sổ Hard Disk Selector, nhấn Add và chọn file Server.vdi đã download ở bước 1 để thêm vào danh sách



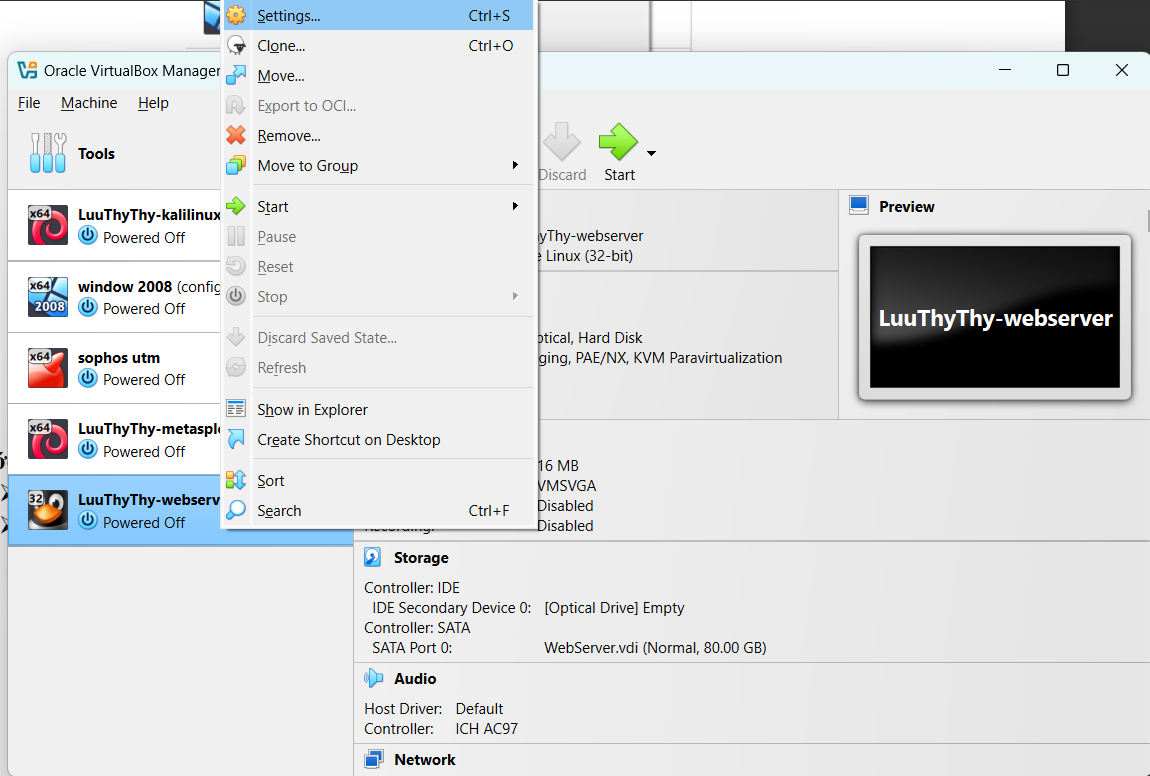




Bước 18: Chọn file Server.vdi vừa được thêm vào trong danh sách ổ cứng ảo. Nhấn Choose để lựa chọn và đóng cửa sổ.

Bước 19: Trên cửa sổ Hard disk, nhấn Create để tạo ổ cứng ảo.

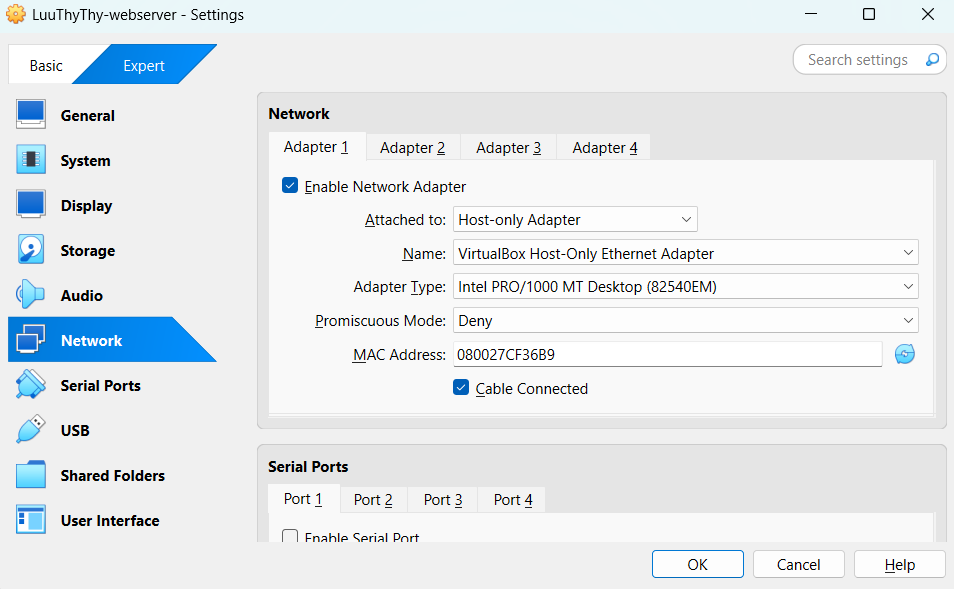
Bước 20: Trên cửa sổ chính của Virtualbox, chọn máy ảo vừa tạo và nhấp chuột phải. Chọn Settings...



Bước 21: Chọn Network → Adapter 1. Thiết lập các thông số như sau:

➢ Attached to: Host-only Adapter

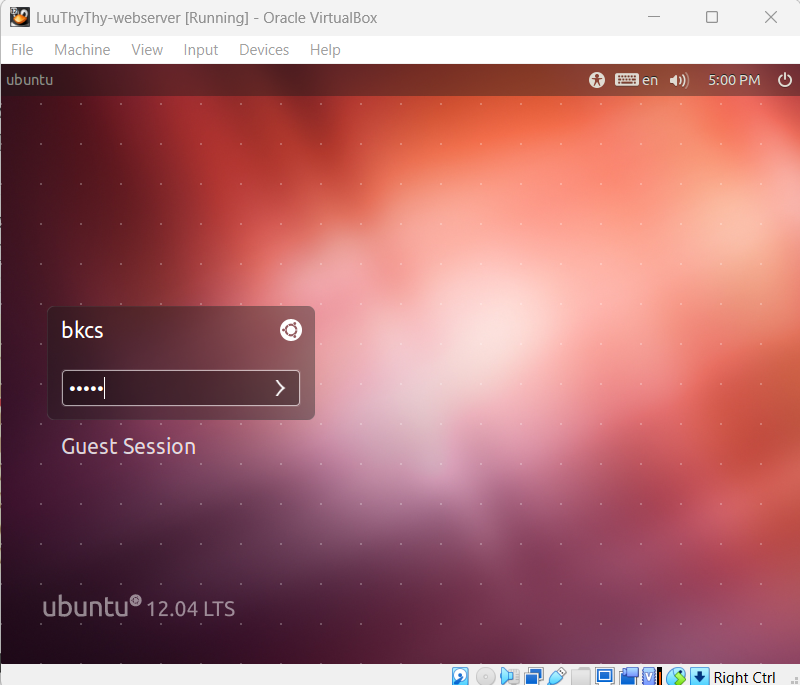
➢ Name: VirtualBox Host-Only Ethernet Adapter (hoặc còn gọi là VirtualBox Host-Only Network)



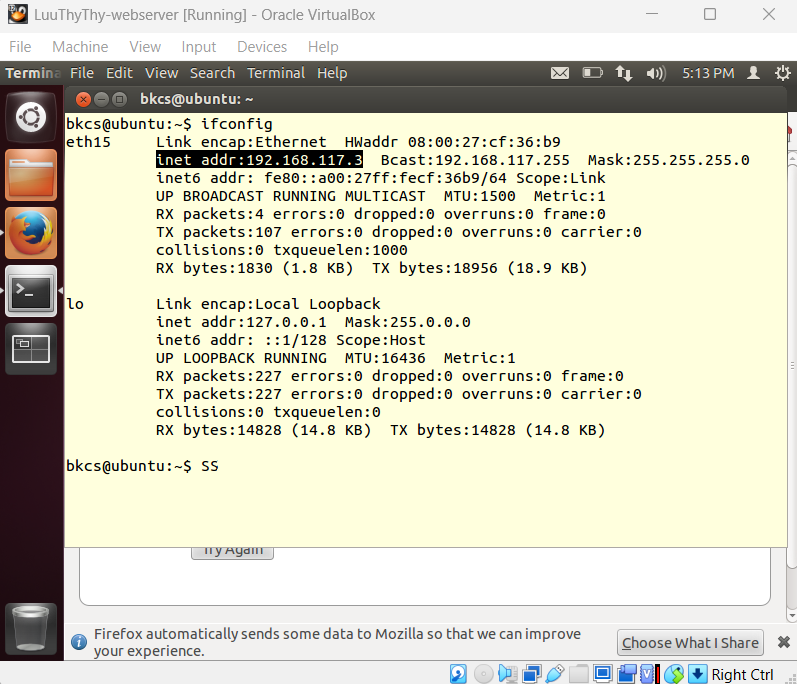
Sau khi máy ảo khởi động xong, đăng nhập bằng tài khoản sau:

➢ Username: bkcs

➢ Password: bkcs

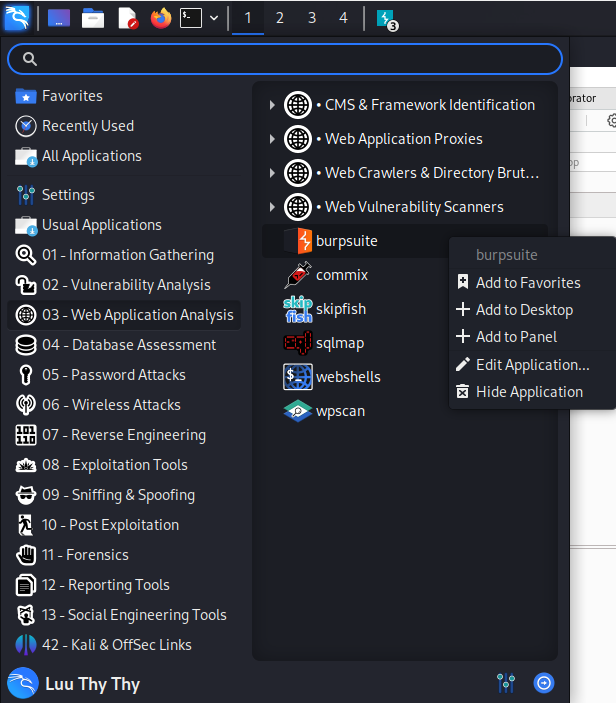


Khi thực hiện các nội dung luyện tập trong tài liệu hướng dẫn bài thực hành số 5 và số 6, địa chỉ localhost khi truy cập vào các trang Web được thay thế bằng địa chỉ IP của Web Server. Trên Web Server mở cửa sổ Terminal và thực hiện lệnh ifconfig. Trong hình ảnh minh họa sau, địa chỉ của Web Server là 192.168.117.24

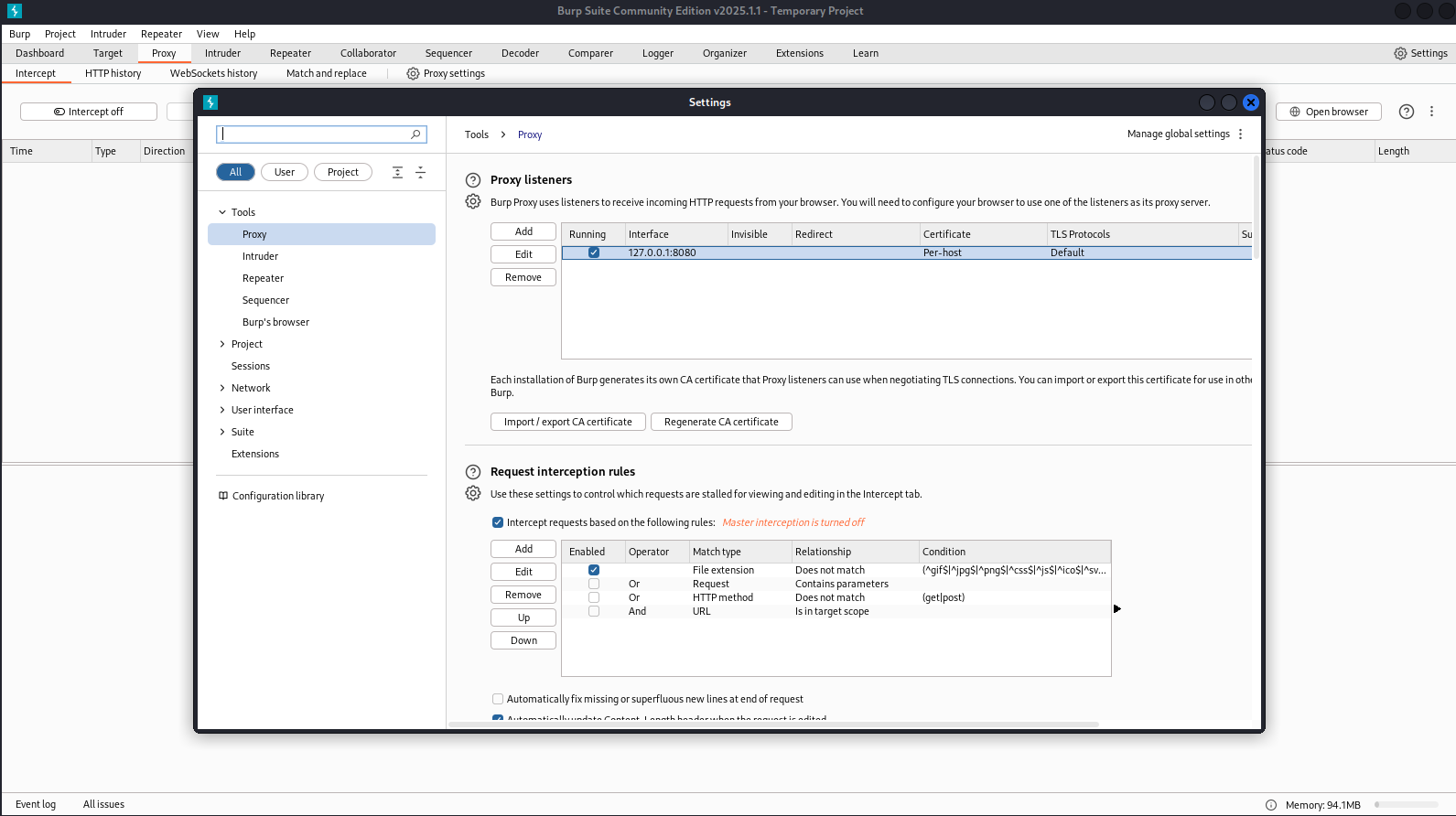


Sử dụng công cụ hỗ trợ kiểm thử Burpsuite

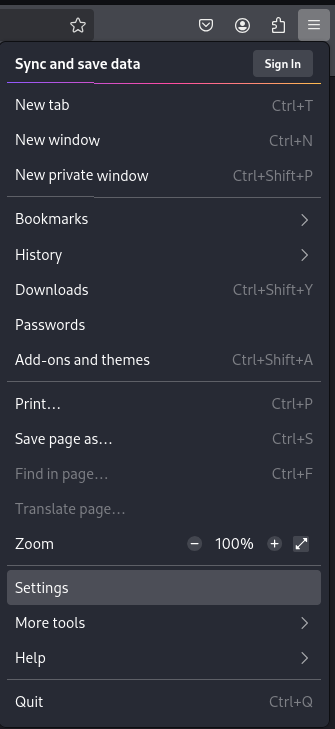
Truy cập burpsuite trên máy ảo

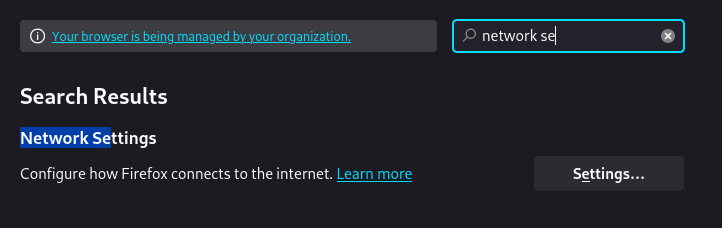


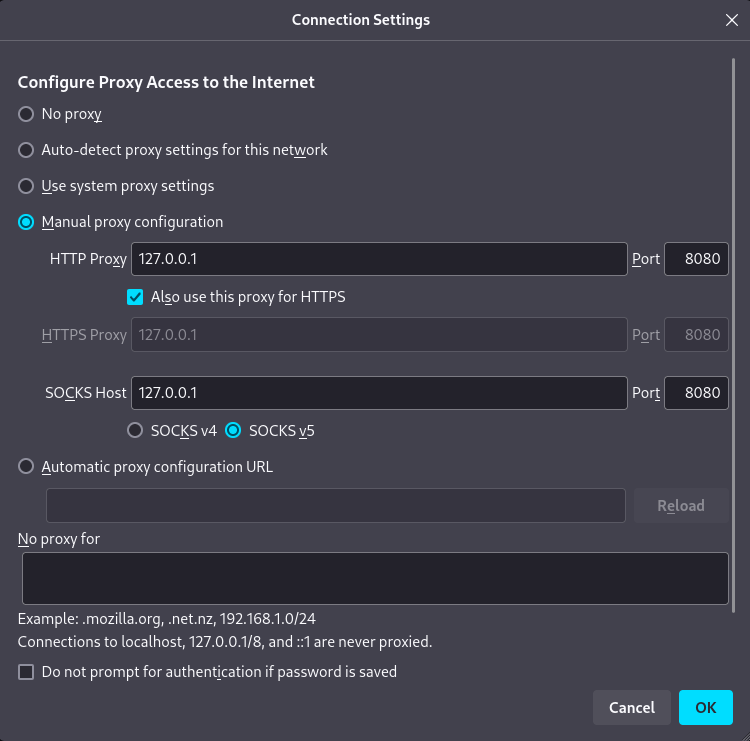
Theo mặc định, Burp Proxy được cấu hình lắng nghe trên cổng 8080/TCP. Để kiểm tra chắc chắn rằng không có chương trình hoặc dịch vụ nào khác đang lắng nghe trên cùng cổng 8080/TCP, bạn thực hiện kiểm tra tại thẻ Proxy | Options.



Thực hiện cấu hình Proxy tại trình duyệt Firefox như ảnh minh họa





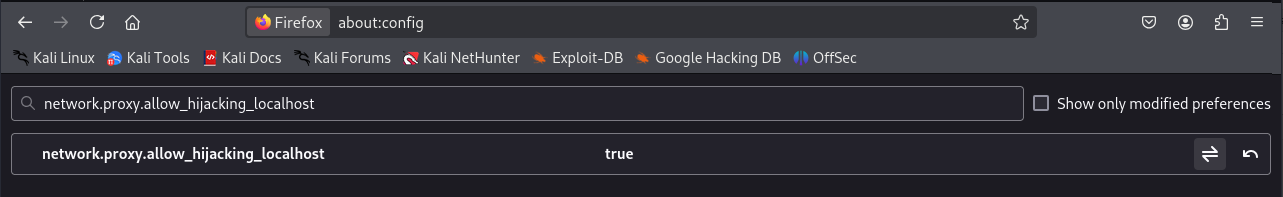


Thiết lập cấu hình để cho phép proxy hoạt động với các các lưu lượng cục bộ (localhost):

Bước 1: Mở một tab mới và truy cập tới trang about:config. Bỏ qua các cảnh báo nếu có



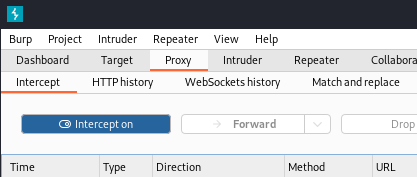
Bước 2: Điền giá trị network.proxy.allow\_hijacking\_localhost vào ô tìm kiếm và thiết lập giá trị true cho nó



Sử dụng Burpsuite hỗ trợ kiểm thử SQL Injection

Bước 1: Cấu hình và khởi động Burpsuite như hướng dẫn ở phần trước

Bước 2: Trên cửa sổ công cụ Burpsuite, mở thẻ Proxy → Intercept và chắc chắn tính năng Interceptis on đã được bật

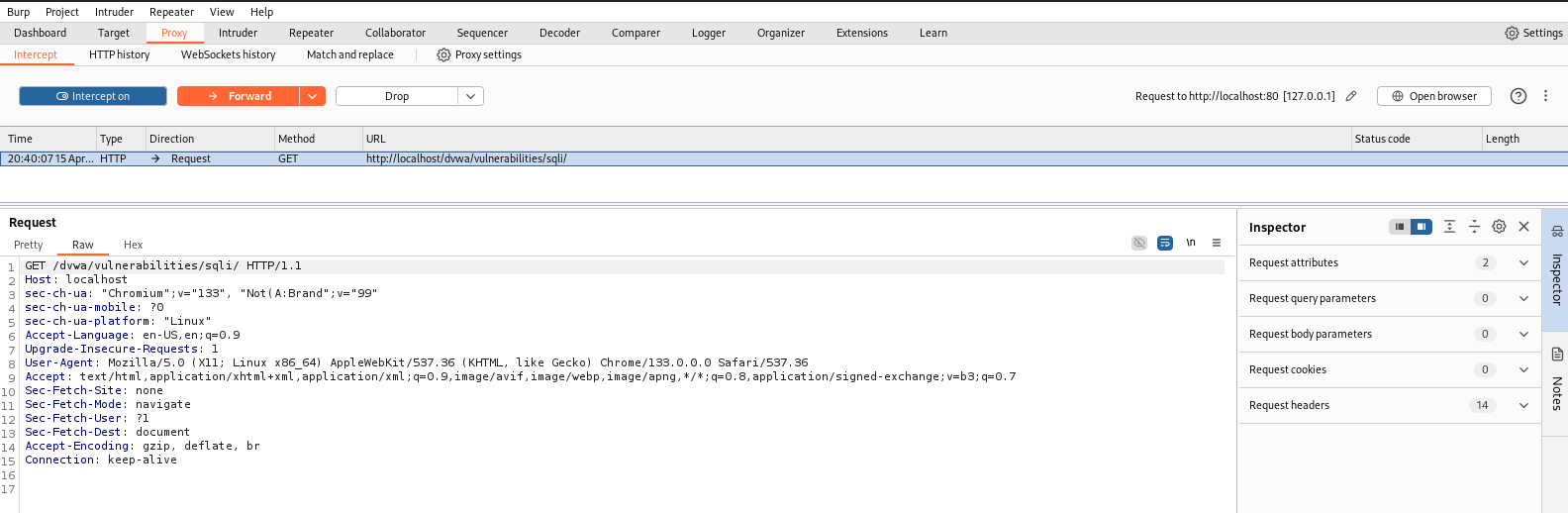


Bước 3: Mở địa chỉ trang Web cần kiểm thử. Ví dụ dưới đây là giao diện kiểm tra lỗ hổng SQLInjecion trên website DVWA.

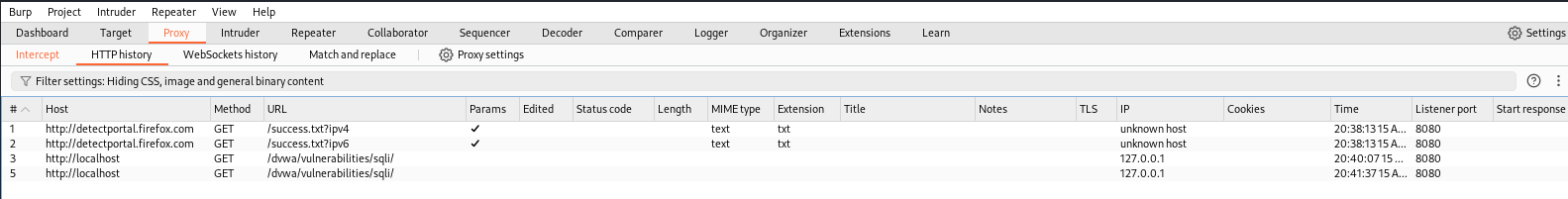
<http://localhost/dvwa/vulnerabilities/sqli/>

Bước 4: Điền các giá trị bất kỳ nào đó và gửi yêu cầu từ trình duyệt

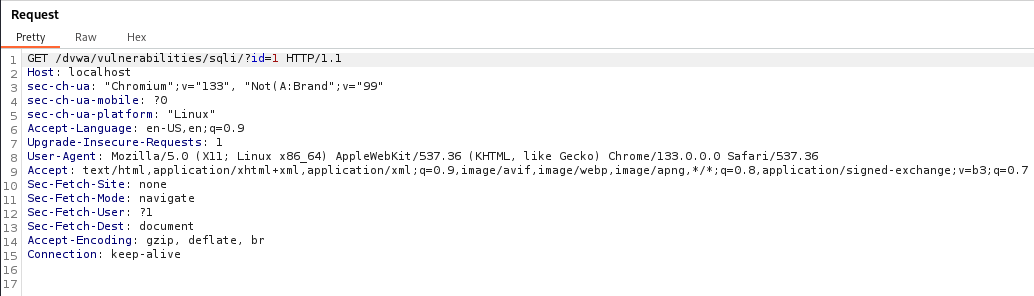
Bước 5: Trên thẻ Proxy → Intercept, nhấn nút Forward để chuyển tiếp yêu cầu

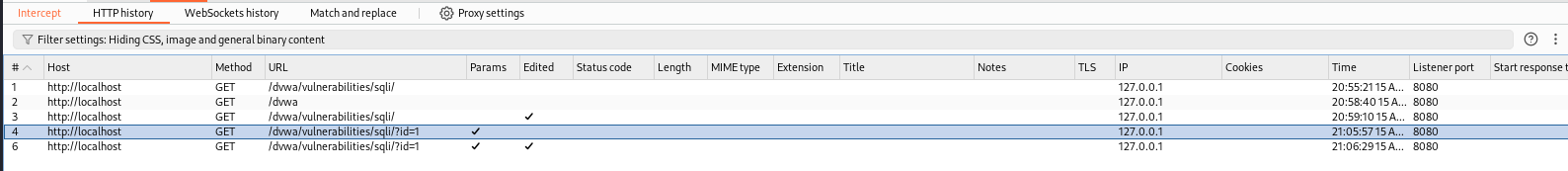


Bước 6: Mở thẻ Proxy → HTTP history, chúng ta sẽ thấy danh sách các thông điệp HTTP mà Burpsuite đã bắt được. Chọn thông điệp HTTP Request tương ứng ở bước 4, nhấn chuột phải và chọn Send to Repeater



Bước 7: Chọn thẻ Repeater. Thẻ này cho phép chúng ta thay đổi nội dung của HTTP Request và phát lại tới máy chủ. Thẻ con Params liệt kê danh sách các giá trị trên HTTP Header có thể là tham số đầu vào.

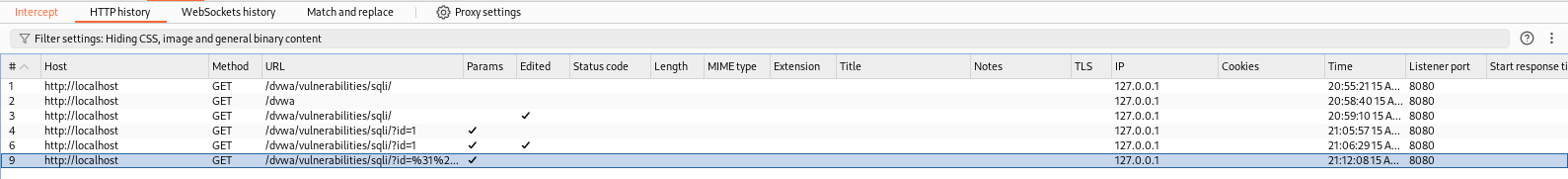




Bước 8: Để thực hiện kiểm thử cho tham số đầu vào id chúng ta sẽ sửa trực tiếp trên thẻ con Raw. Chọn thẻ Decoder, điền chuỗi 1' or 1;# và chọn Encode as...→ URL. Kết quả encode cho chúng ta xâu %31%27%20%6f%72%20%31%3b%23. Chọn lại thẻ Repeater, thay xâu giá trị này vào cho tham số id và nhấn nút Go. Thông điệp HTTP Response trả về từ server được hiển thị theo nhiều dạng khác nhau trong phần Response.

(Giá trị các tham số cũng có thể sửa trực tiếp từ thẻ Params mà không cần qua encode)

****

****