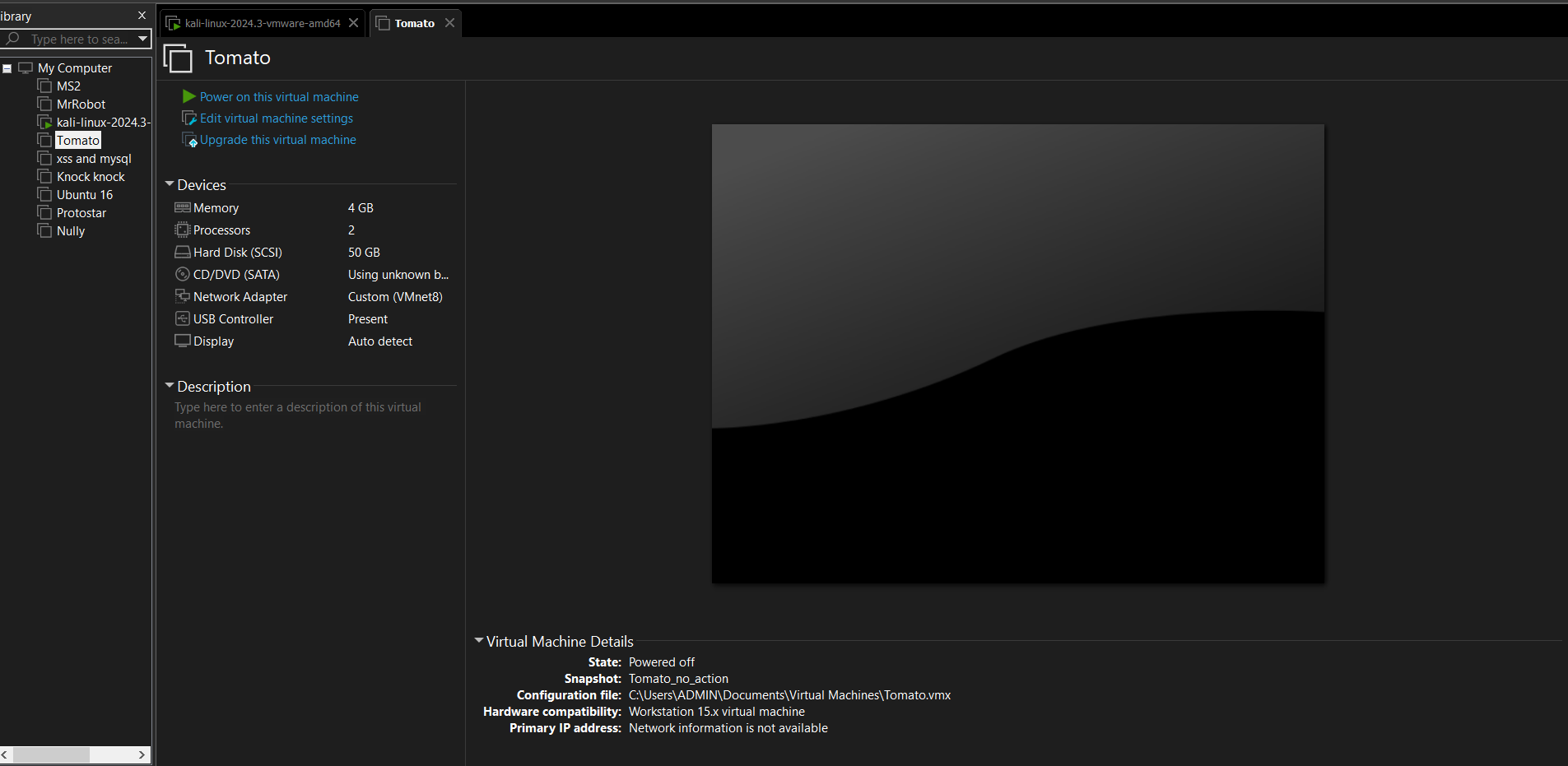
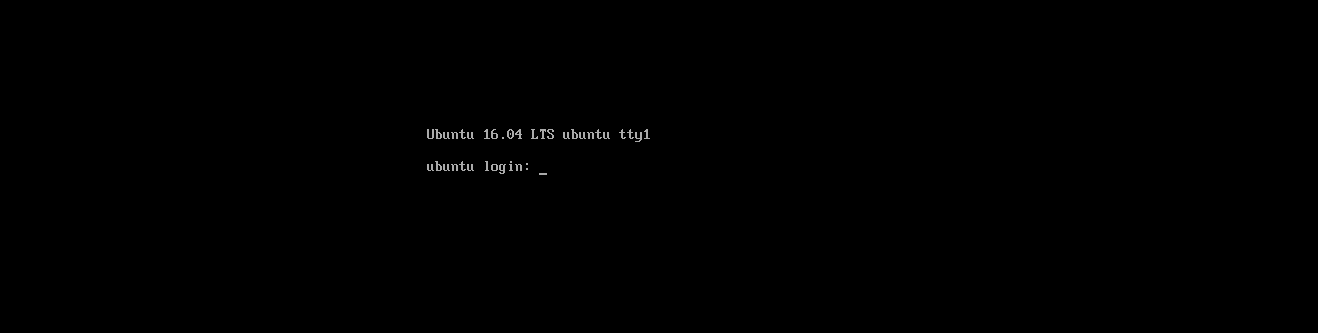
# TOMATO WRITE UP (VULHUB)

# 1. Chuẩn bị

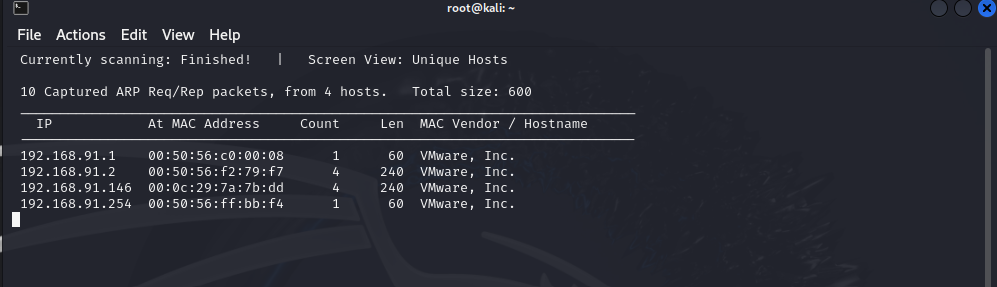
Tải máy ảo về và cài đặt theo hướng dẫn:



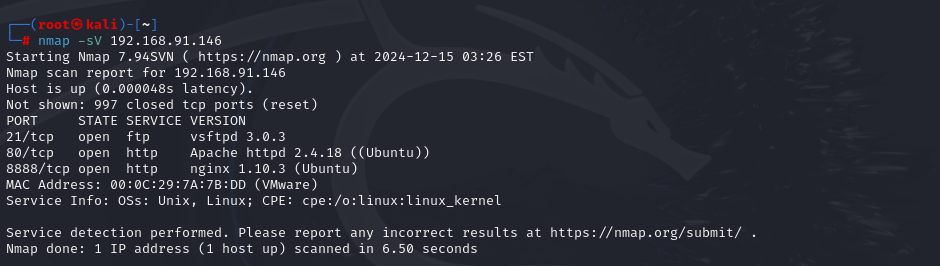
Chạy máy ảo và đợi khoảng 5-8 phút



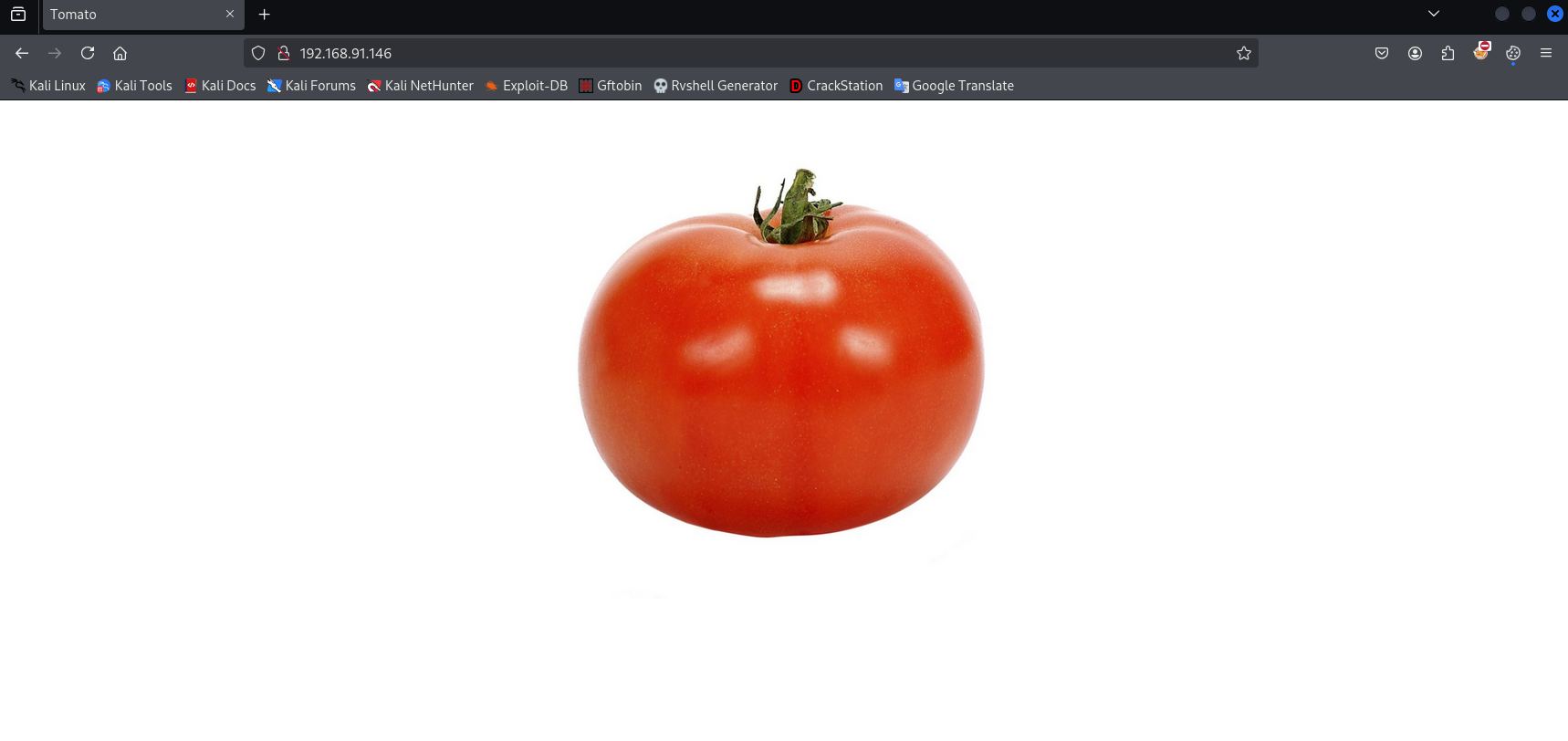
Trên máy tấn công, sử dụng netdiscover để quét các host đang hoạt động trên dải mạng, tìm ra IP máy ảo là 192.168.91.146



Check nhanh bằng nmap để kiểm tra các dịch vụ đang chạy trên máy ảo (192.168.91.146)



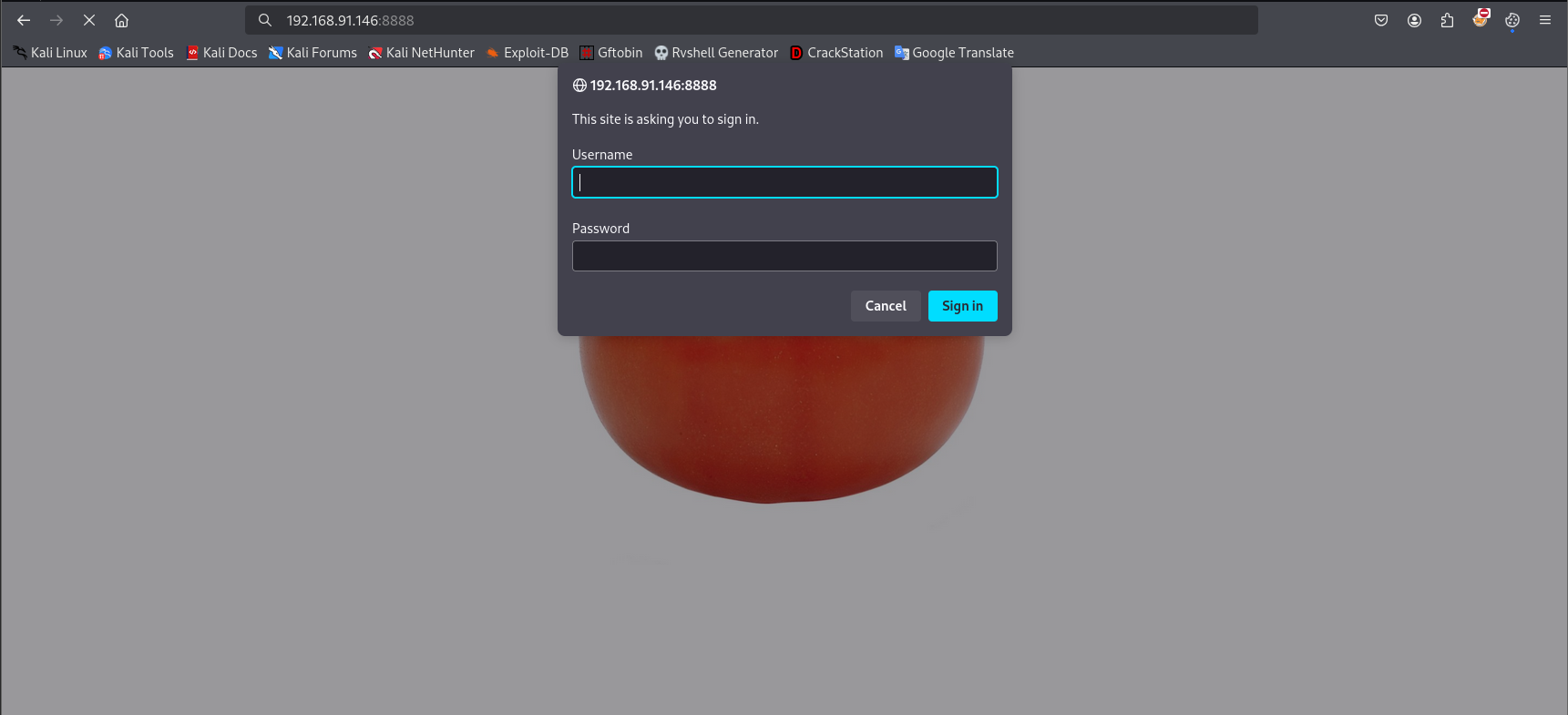
Chạy Web Server trên firefox



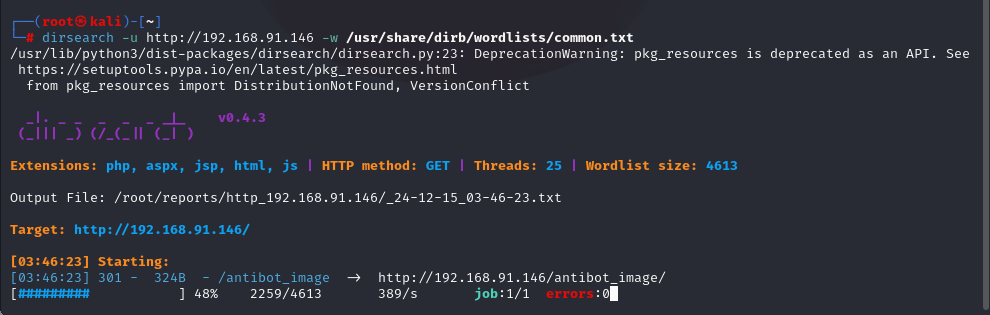
Thông qua nmap, ta thấy rằng cổng 21, 80, 2211, 8888 được mở với các dịch vụ FTP, HTTP, SSH và HTTP tương ứng. Truy cập trang web trên cổng 80 và tìm thấy hình ảnh quả cà chua. Sau khi kiểm tra nhanh mã nguồn, không thấy có gì đặc biệt.

# 2. Khai thác

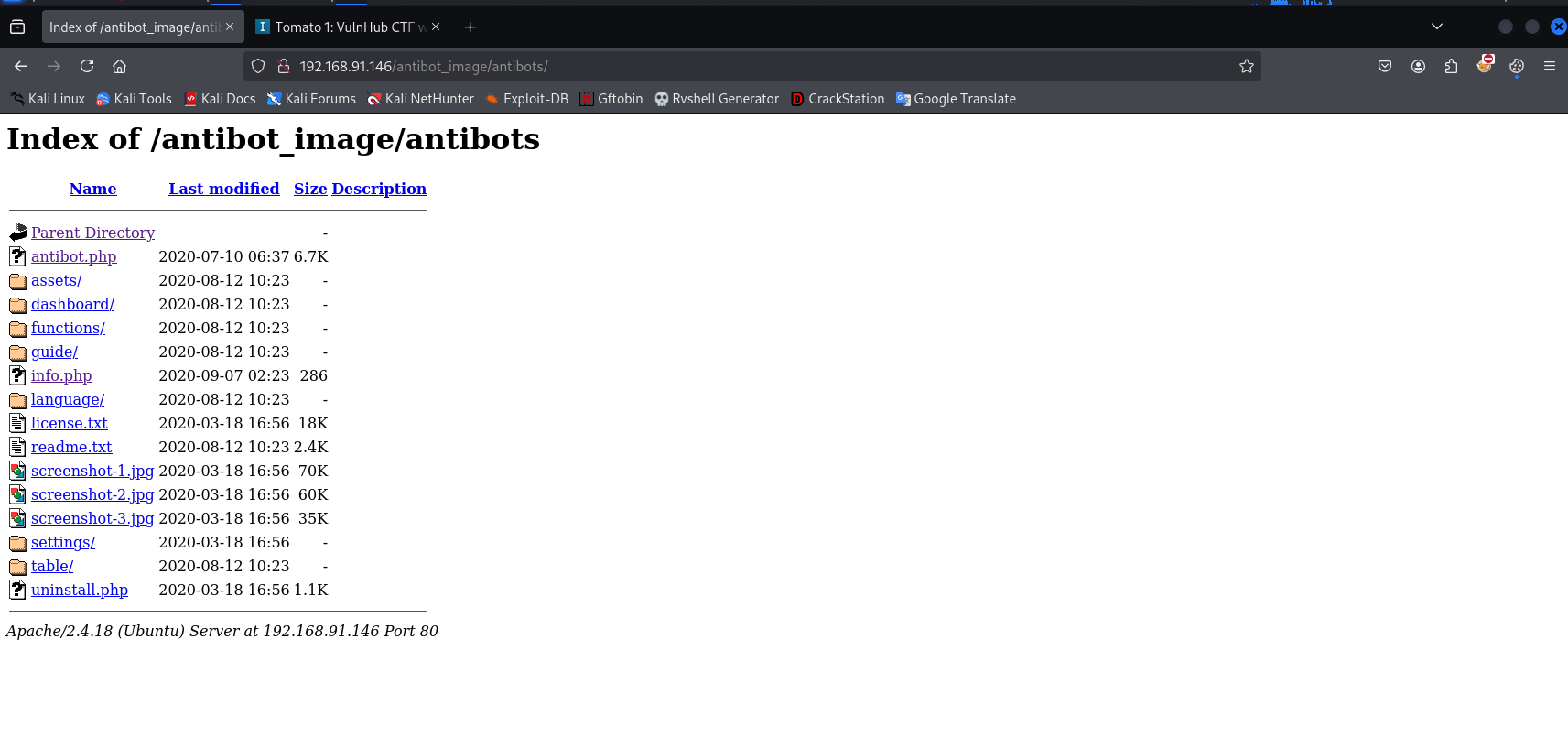
Khi truy cập cổng 8888 ta thấy có yêu cầu đăng nhập ở đây



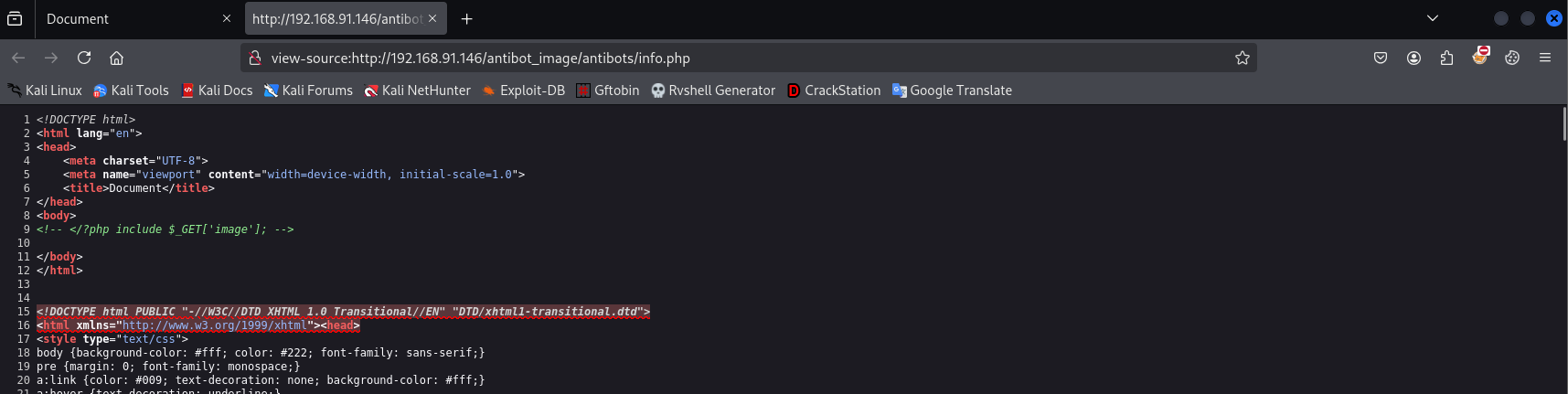
Sử dụng công cụ dirsearch để dò quét thư mục mở rộng và tìm thấy /antibot\_image.



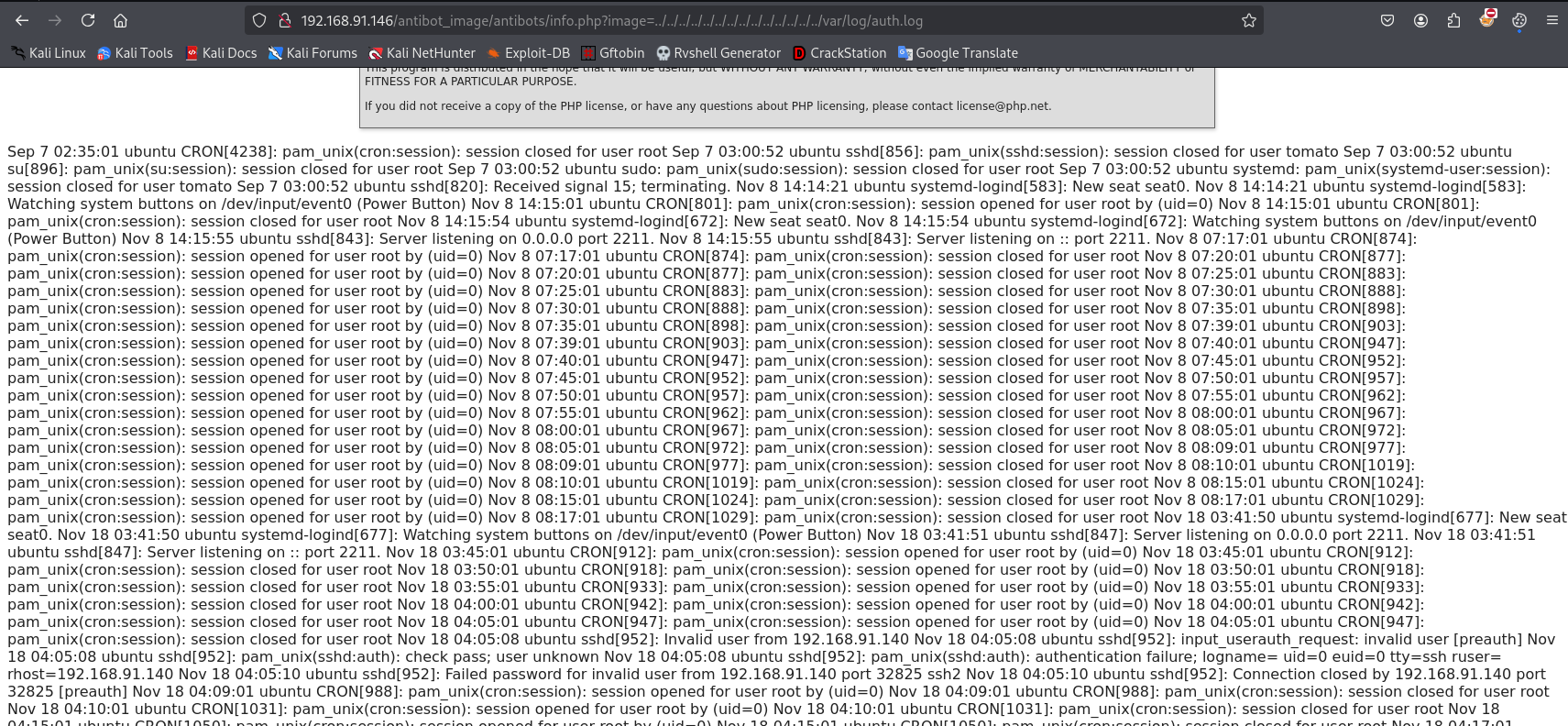
Chúng ta kiểm tra thư mục đã tìm được và tìm thấy danh sách các thư mục



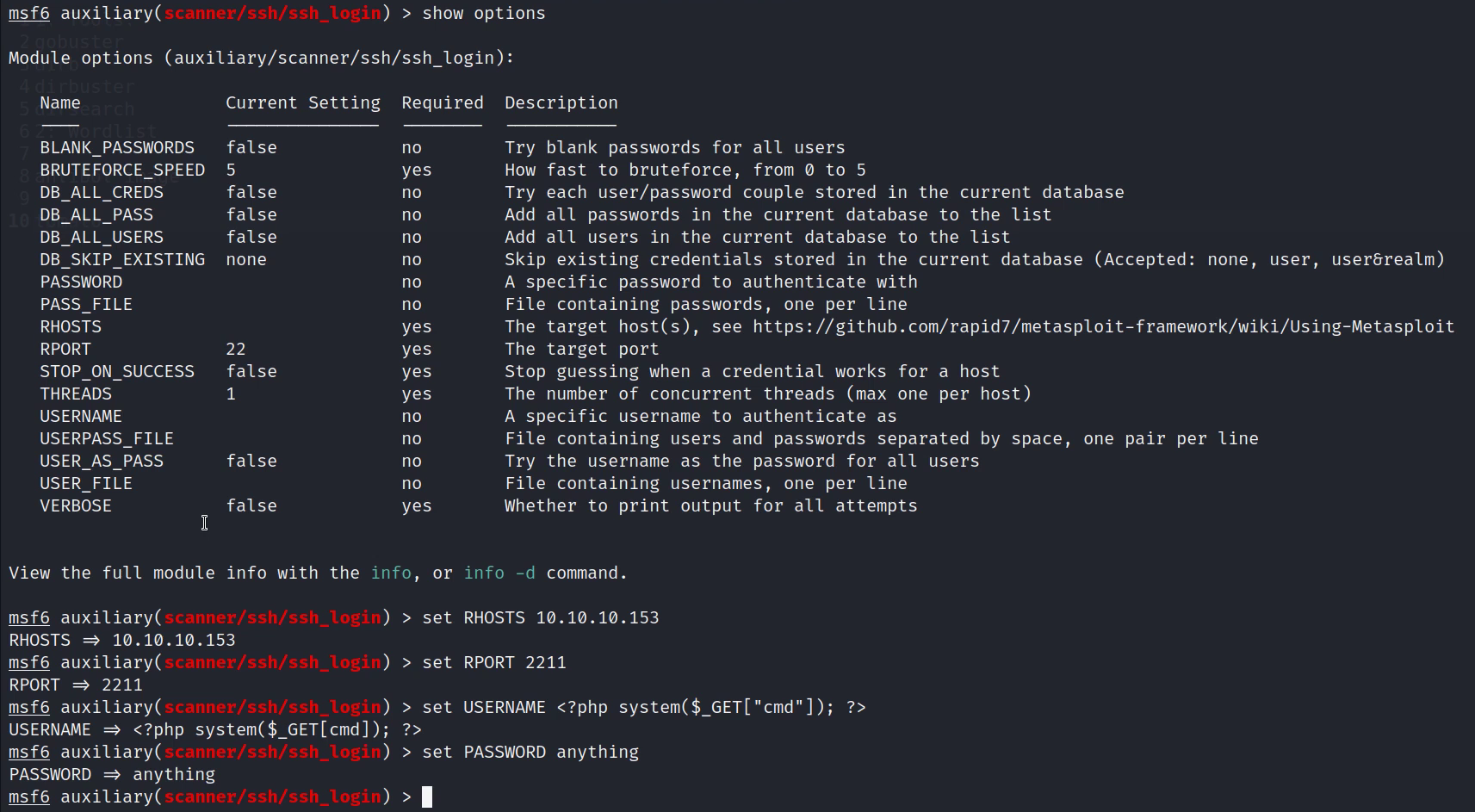
Sau khi kiểm tra các tập tin, chúng ta tìm thấy “ **info.php** ”, ngoài việc hiển thị thông tin hệ thống, phiên bản, v.v. Nó còn bao gồm một dấu hiệu của lỗ hổng lfi.



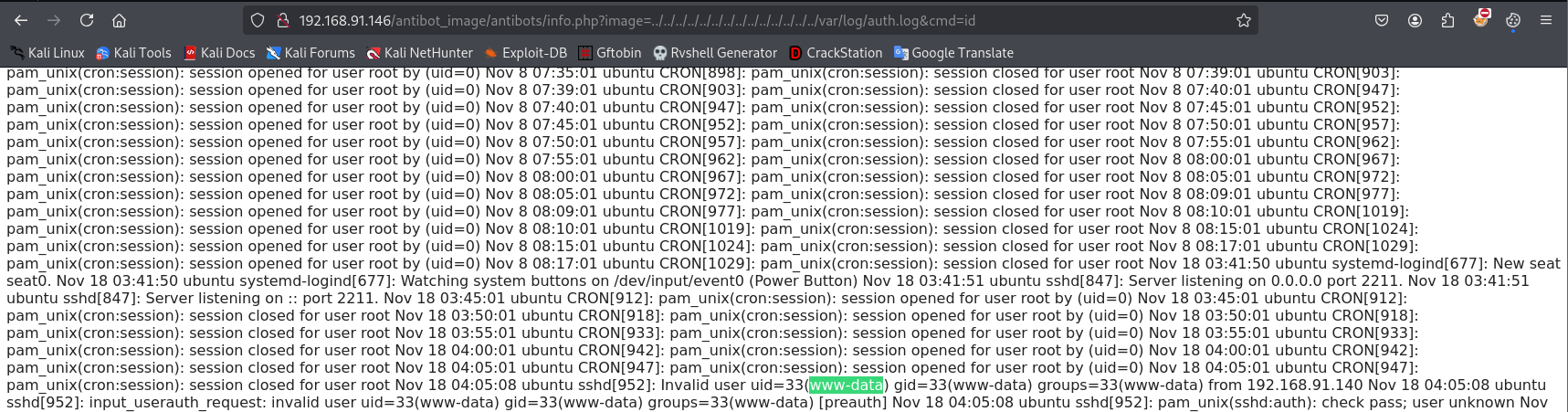
Thử tìm kiếm file log xác thực(auth.log) ta tìm thấy



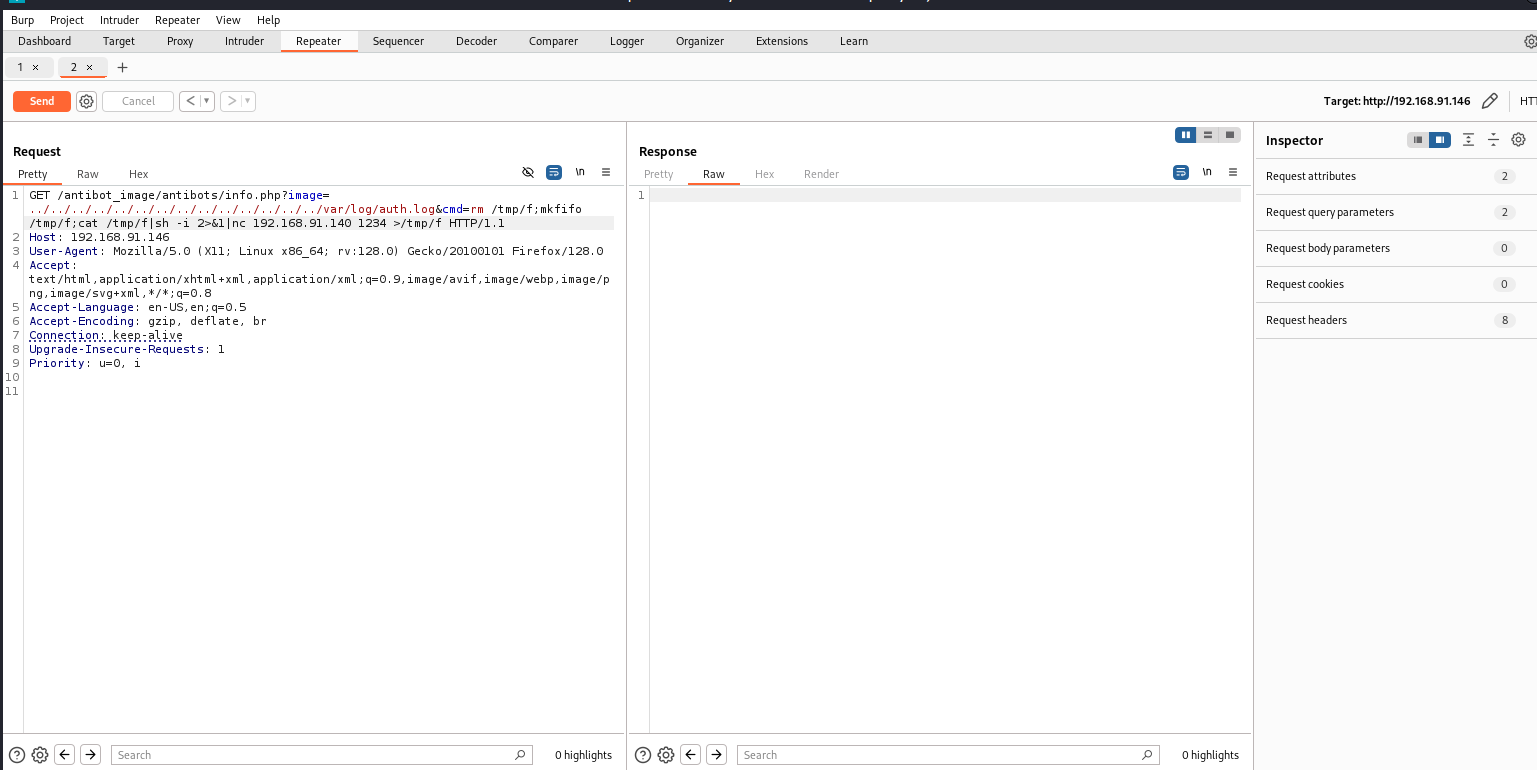
Sử dụng msfconle để gửi một lệnh php để có thể thực thi lệnh từ xa



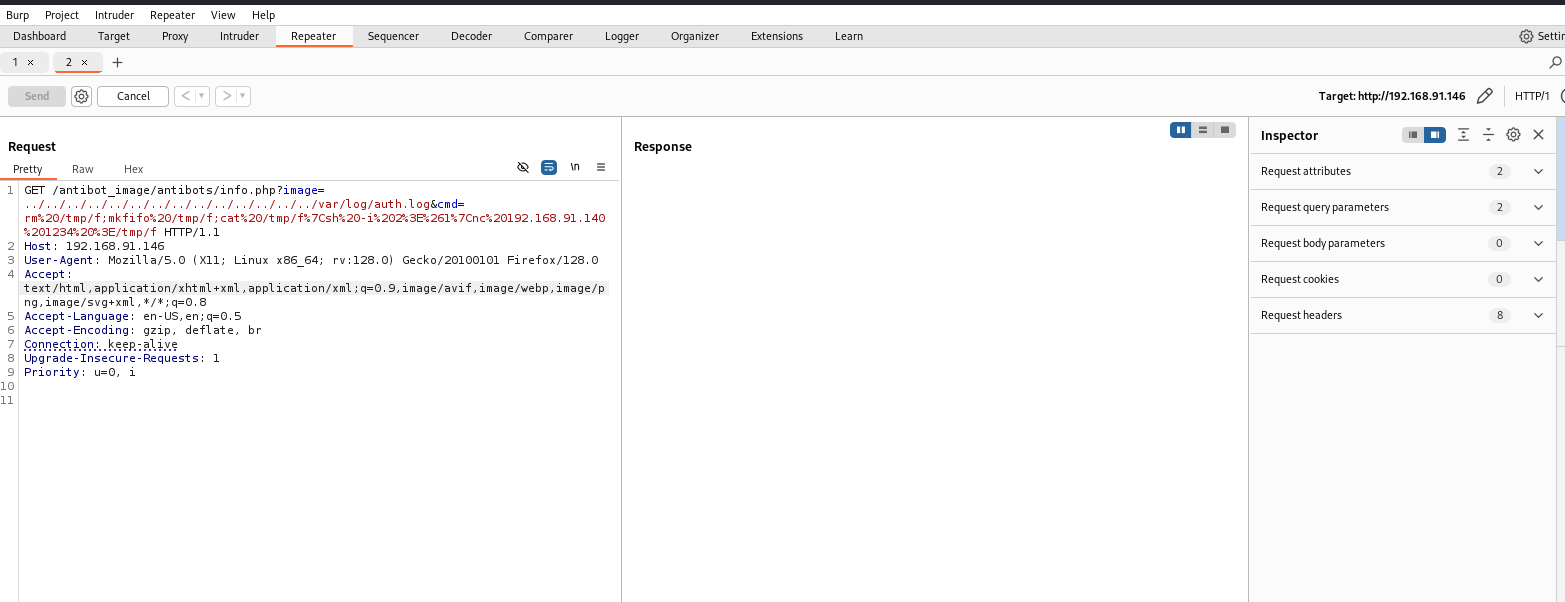
Thành công



Bây giờ chúng ta chèn một reverse shell để truy cập vào máy



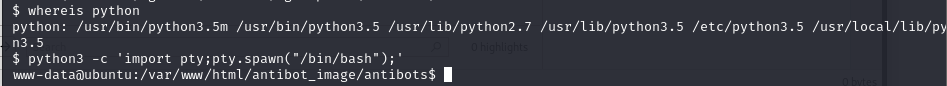
Sử dụng url encode all character để có thể chạy được



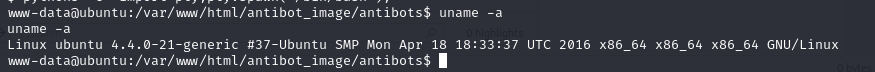
Sử dụng netcat để lắng nghe trên cổng 1234, và chúng ta lấy được shell



Sử dụng python pty để nâng cấp shell



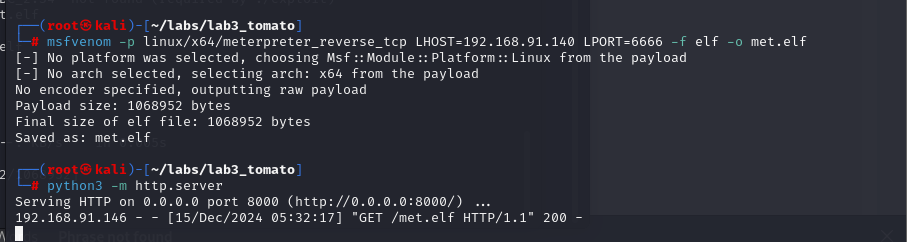
Sử dụng lệnh **uname -a** trong để hiển thị thông tin chi tiết về hệ điều hành và nhân (kernel) đang được sử dụng trên hệ thống. Kernel **4.4.0-21-generic** cho thấy hệ thống đang chạy một phiên bản kernel khá cũ, có thể dễ bị tấn công nếu các bản vá bảo mật không được cập nhật.



Ở đây chúng ta tìm được **CVE-2017-16995** [**https://www.exploit-db.com/exploits/45010**](https://www.exploit-db.com/exploits/45010) trên exploitdb với Linux Kernel < 4.13.9

Sử dụng metasploit để khai thác

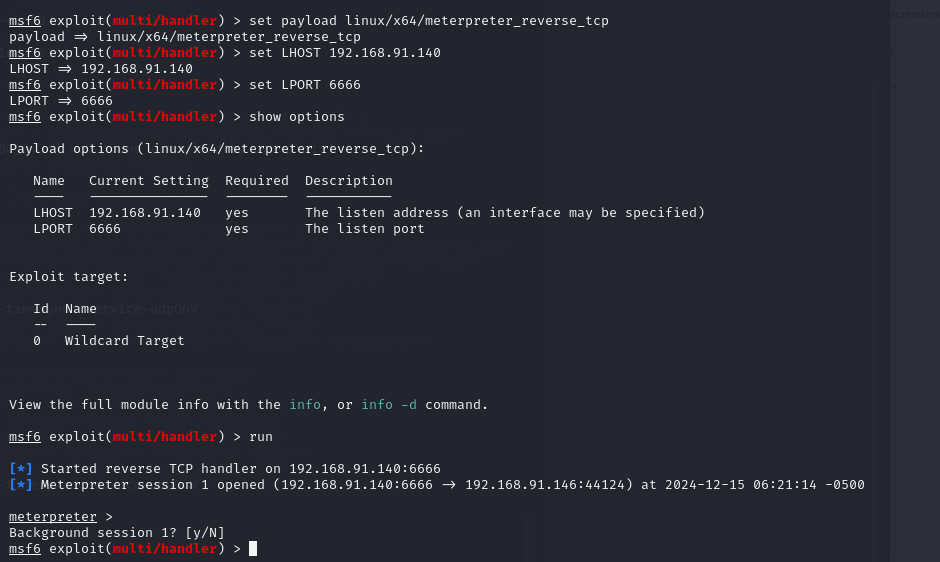
tạo ra một payload (mã độc) cho hệ điều hành **Linux** có kiến trúc **x64**, sử dụng **Meterpreter reverse TCP shell**. Payload này sẽ kết nối lại tới máy của bạn (LHOST) khi được thực thi trên máy mục tiêu, cho phép bạn thực hiện các lệnh từ xa.



Tải payload trên máy victim



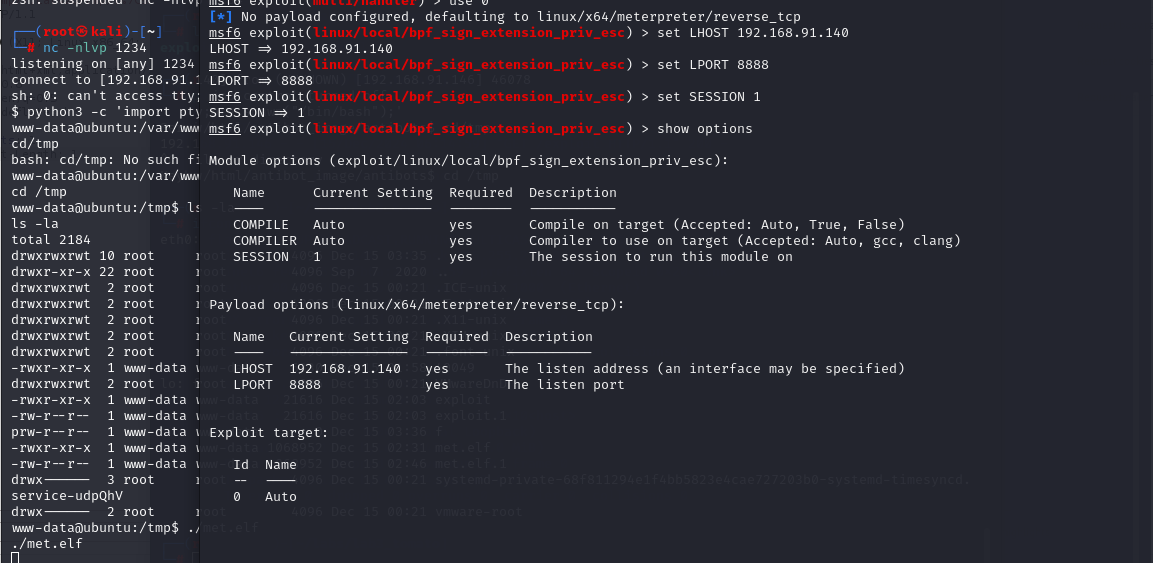
Trên máy attacker sử dụng module exploit/multi/handler của metasploit để chờ kết nối từ mục tiêu và thiết lập session sau khi payload được kích hoạt trên máy mục tiêu, và chúng ta đã nhận được shell metepreter, thiết lập session 1



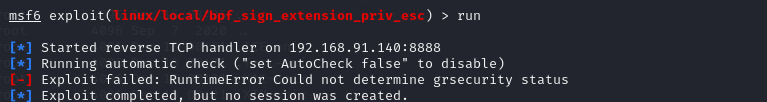
Sử dụng module khai thác với CVE-2017-16995



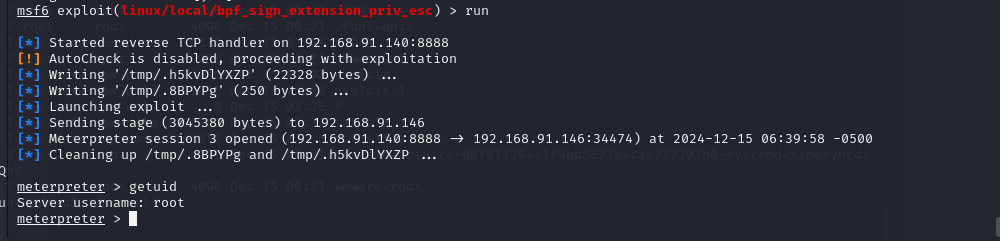
Thiết lập options cho module, LHOST là địa chỉ ip máy attacker, LPORT là cổng đang rảnh trên máy attacker, SESSION là session chúng ta vừa thiết lập với metepreter shell.



Sau đó chạy với lệnh run, trước khi chạy thiết lập AutoCheck = flase nếu không sẽ bị lỗi:



Chúng ta đã có Root:



# 3. Kết quả

Thành công chiếm được quyền root

