|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  **TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG** |
| BÁO CÁO THỰC HÀNH  **TOMATO** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

MỤC LỤC

[Penetration Testing Methodology (phương pháp kiểm thử thâm nhập) 3](#_Toc184490792)

[**I)** **Trinh sát** 3](#_Toc184490793)

[**II)** **Enumeration** 4](#_Toc184490794)

[**III)** **Exploiting** 8](#_Toc184490795)

[Privilege Escalation (root) 14](#_Toc184490796)

# Penetration Testing Methodology (phương pháp kiểm thử thâm nhập)

**Reconnaissance (Trinh sát)**

* Netdiscover
* Nmap

**Enumeration (liệt kê thông tin chi tiết về mục tiêu)**

* Dirsearch

**Exploiting (khai thác)**

* RCE with LFI and SSH Log Poisoning

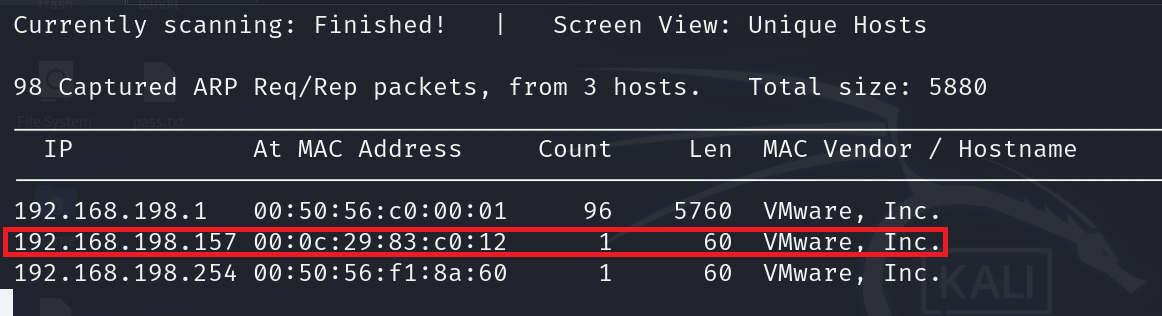
**Privilege Escalation (leo thang đặc quyền)**

* Abuse kernel exploit CVE-2017-16995
* Capture the flag

1. **Trinh sát**

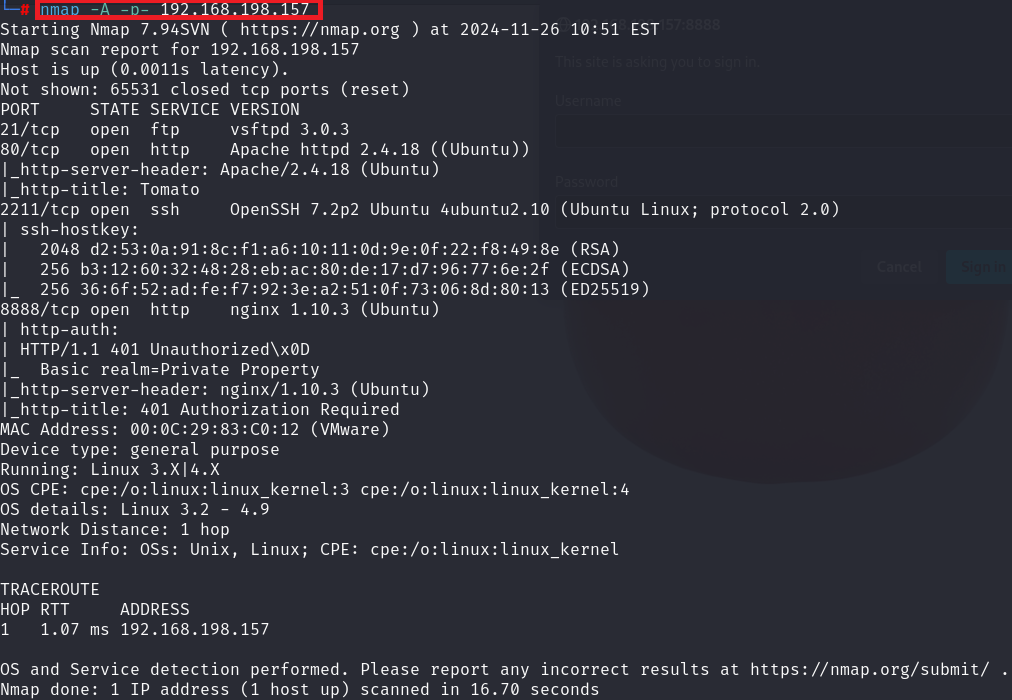
Để xác định địa chỉ IP mục tiêu, chúng ta sẽ chạy lệnh sau:

netdiscover -i eth0 -r 192.168.129.0/24



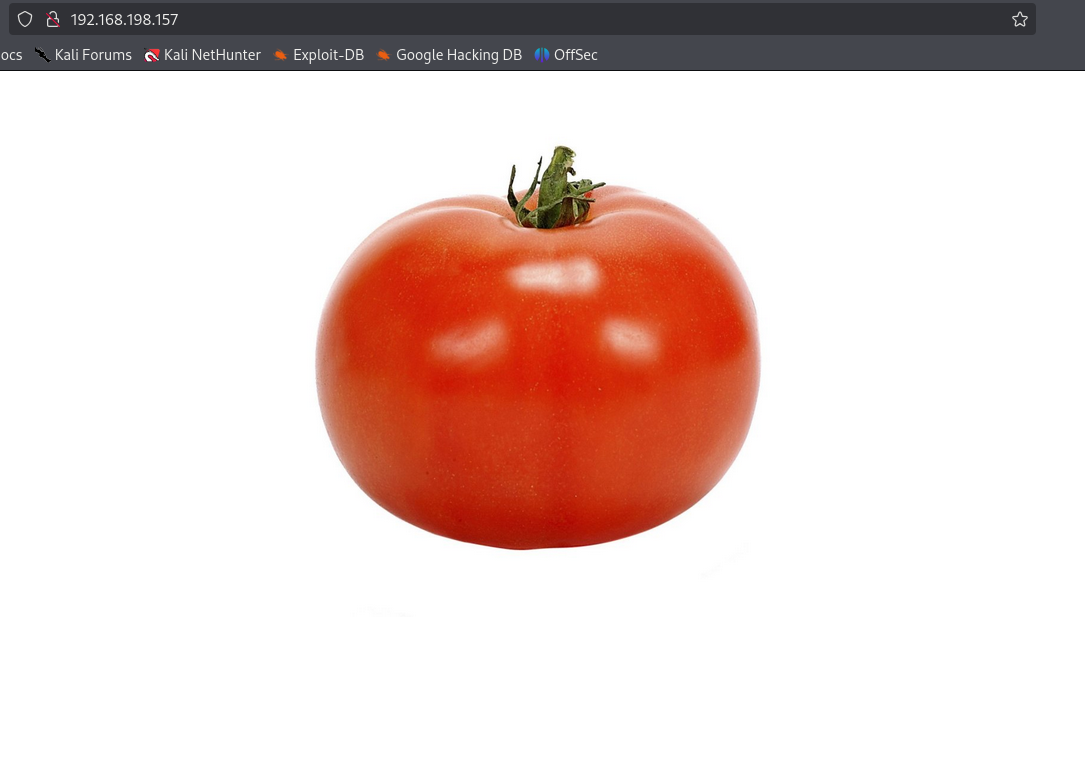
Bây giờ chúng ta sẽ chạy quét mạng bằng nmap để tìm ra cổng nào đang mở và dịch vụ nào chúng chạy. Nmap là một trong những công cụ quét mạng tốt nhất vì nó cung cấp cho chúng ta tất cả thông tin liên quan đến cổng, hệ điều hành, dịch vụ, v.v.

nmap –A –p- 192.168.198.157

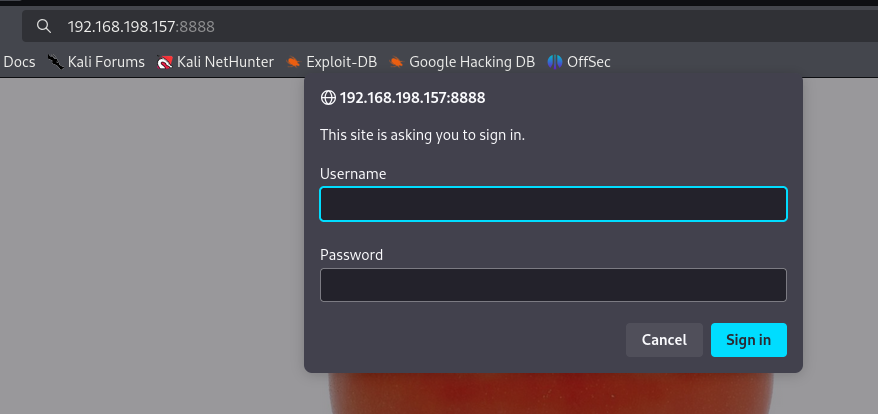


1. **Enumeration**

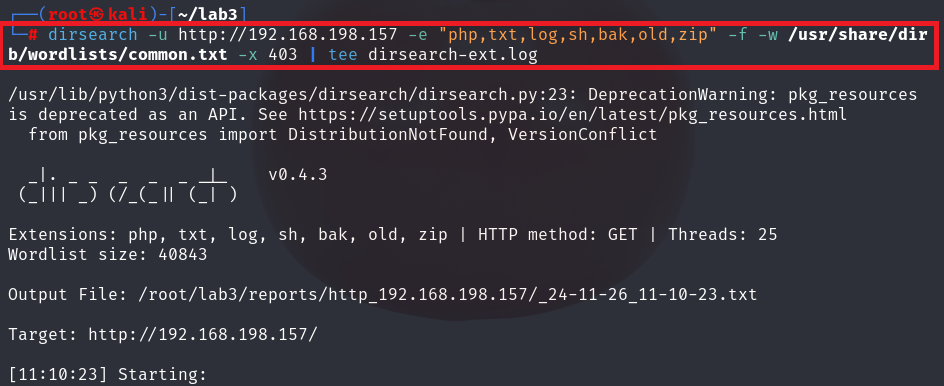
Thông qua nmap, chúng ta biết rằng cổng 21, 80, 2211, 8888 được mở với các dịch vụ FTP, HTTP, SSH và HTTP tương ứng. Chúng ta truy cập dịch vụ web cổng 80 và tìm thấy một trang duy nhất có hình ảnh quả cà chua. Sau khi kiểm tra hình ảnh bằng một số công cụ tốc ký, chúng ta không tìm thấy bất cứ điều gì có thể hữu ích.

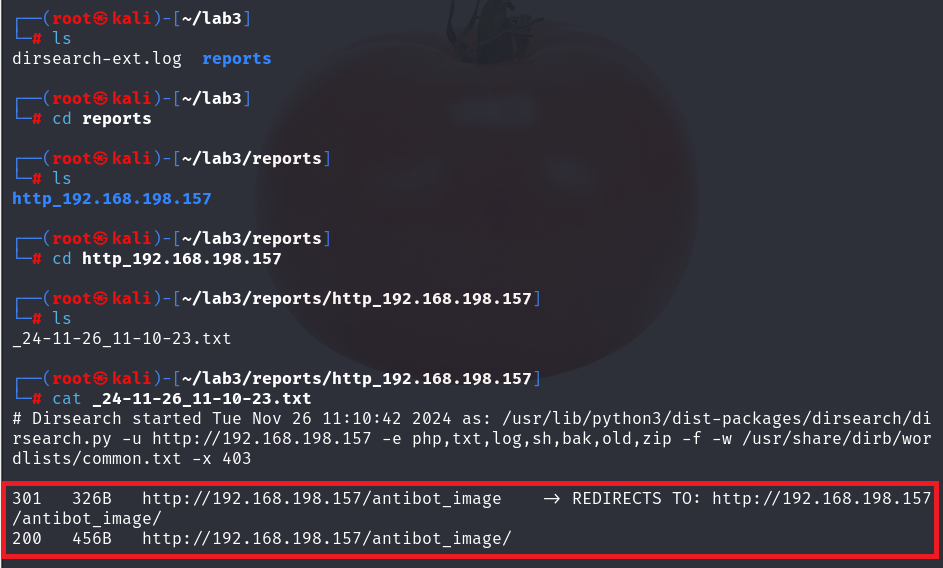


Khi chúng ta truy cập vào cổng 8888, chúng ta tìm thấy một máy chủ Nginx được bảo vệ bằng tên người dùng và mật khẩu.

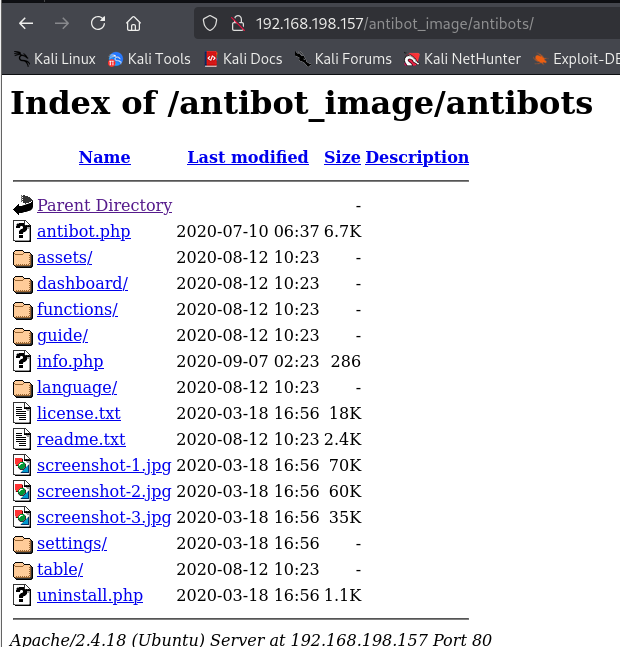


Ở đây, chúng ta sử dụng **dirsearch** với từ điển “**common**” và chỉ định các phần mở rộng điển hình nhất. Chúng tôi tìm thấy thư mục “**/antibot\_image/“.**

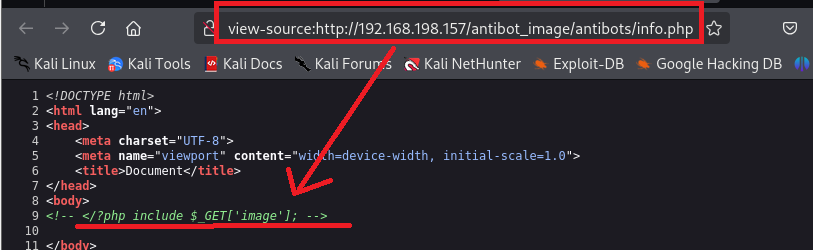




Chúng ta đã kiểm tra thư mục và tìm thấy “Danh sách thư mục”:

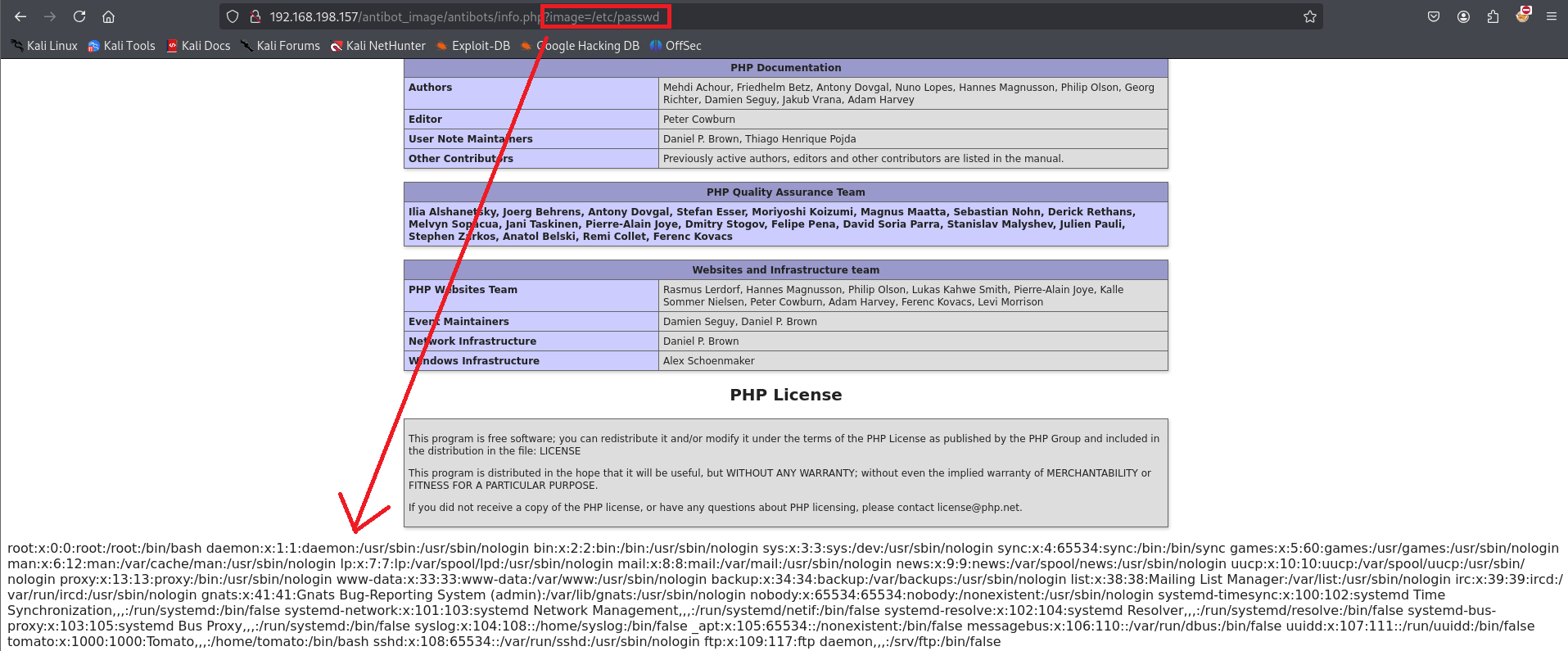


Khi kiểm tra các tập tin, chúng ta tìm thấy “info.php“, ngoài việc hiển thị thông tin hệ thống, phiên bản, v.v., nó còn bao gồm một món quà bên trong. (Có thể đây là phần phức tạp nhất của hộp).



Lỗi này sẽ cho phép chúng ta tải tệp lên qua URL. Hãy cùng thực hiện một proof of concept.

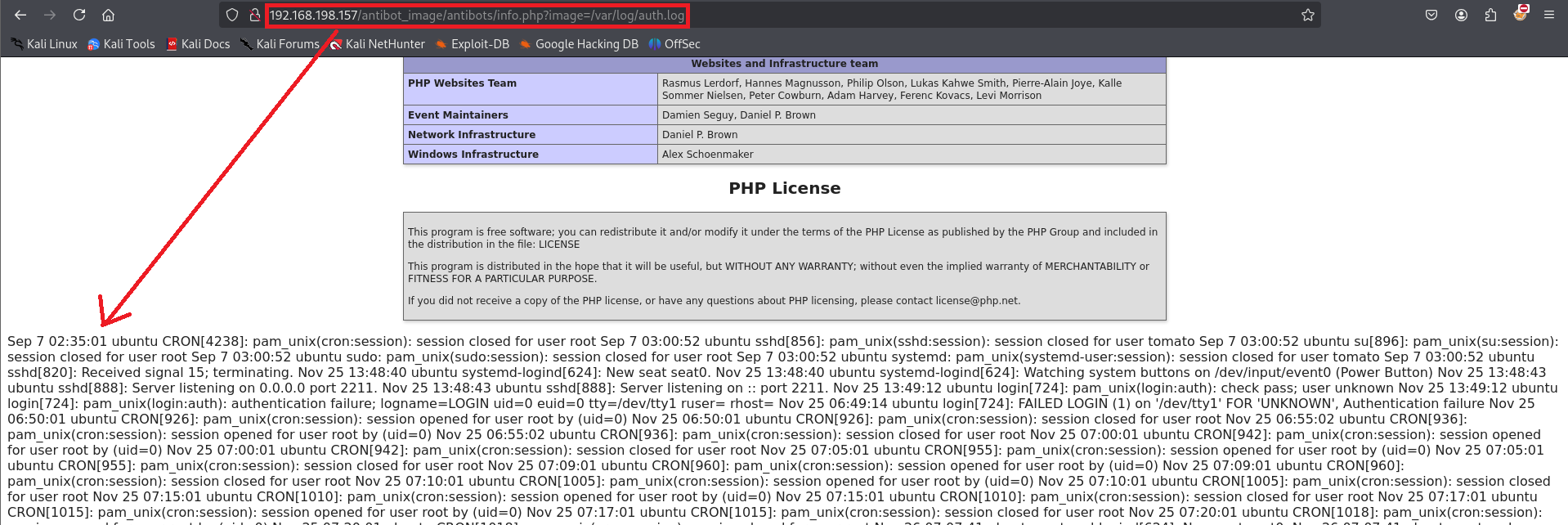
Thêm ?image=/etc/passwd để xem lỗ hổng



Thật vậy! Trang web này dễ bị tấn công bởi LFI (Local File Inclusion).

1. **Exploiting**

Vì chúng ta có thể tải các tệp, hãy thử tải các tệp nhật ký, ví dụ như tệp nhật ký của dịch vụ SSH.

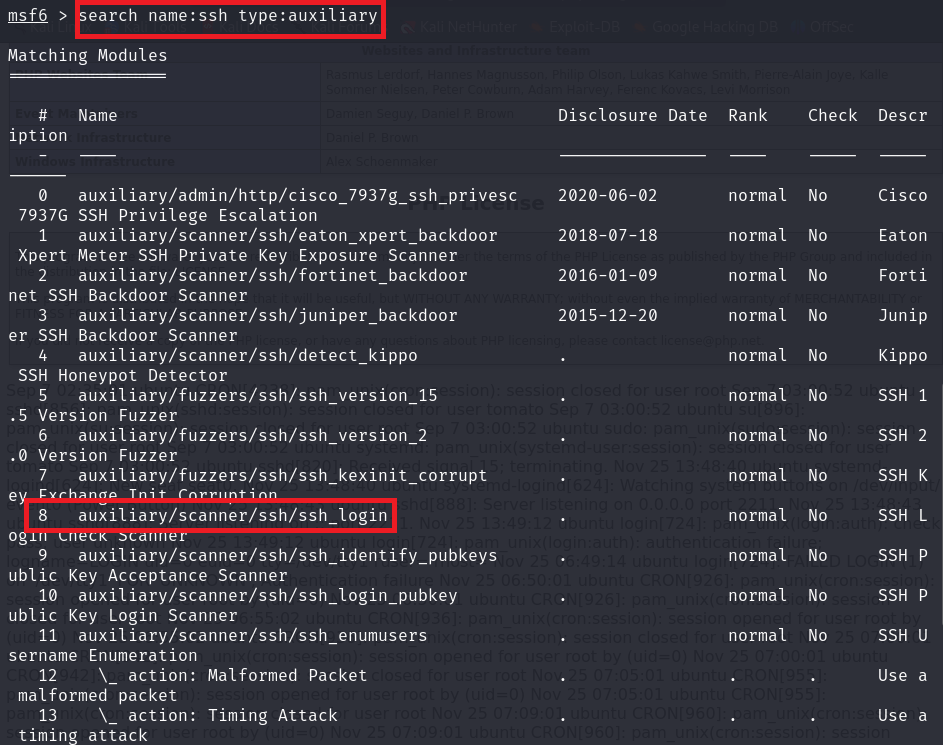


Bây giờ, chúng ta hãy đăng nhập bằng SSH, sau đó chúng ta sẽ thay đổi người dùng bằng mã PHP cho phép chúng ta thực thi các lệnh.

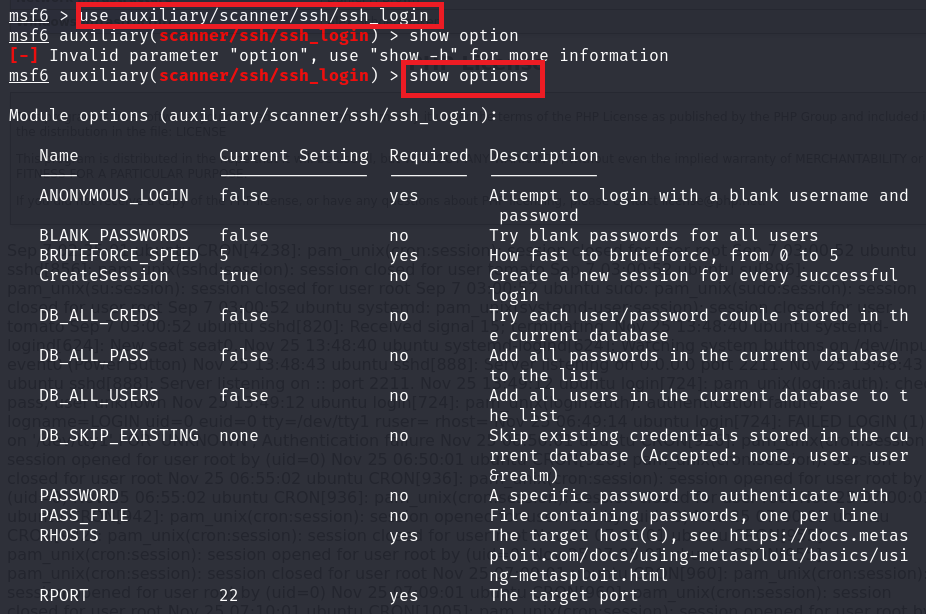


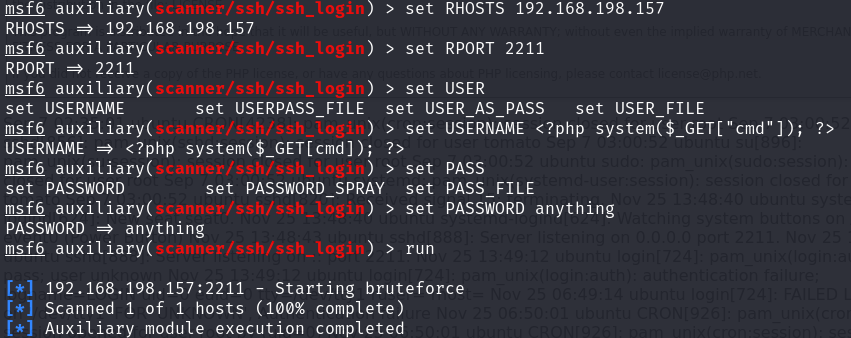
Chúng ta có thể dùng phiên bản linux cũ hơn để thực hiện thành công lệnh này. Tuy nhiên, chúng ta đang dùng phiên bản linux mới hơn nên chúng ta có thể sử dụng msfconsole tool để khai thác

Search modun và type

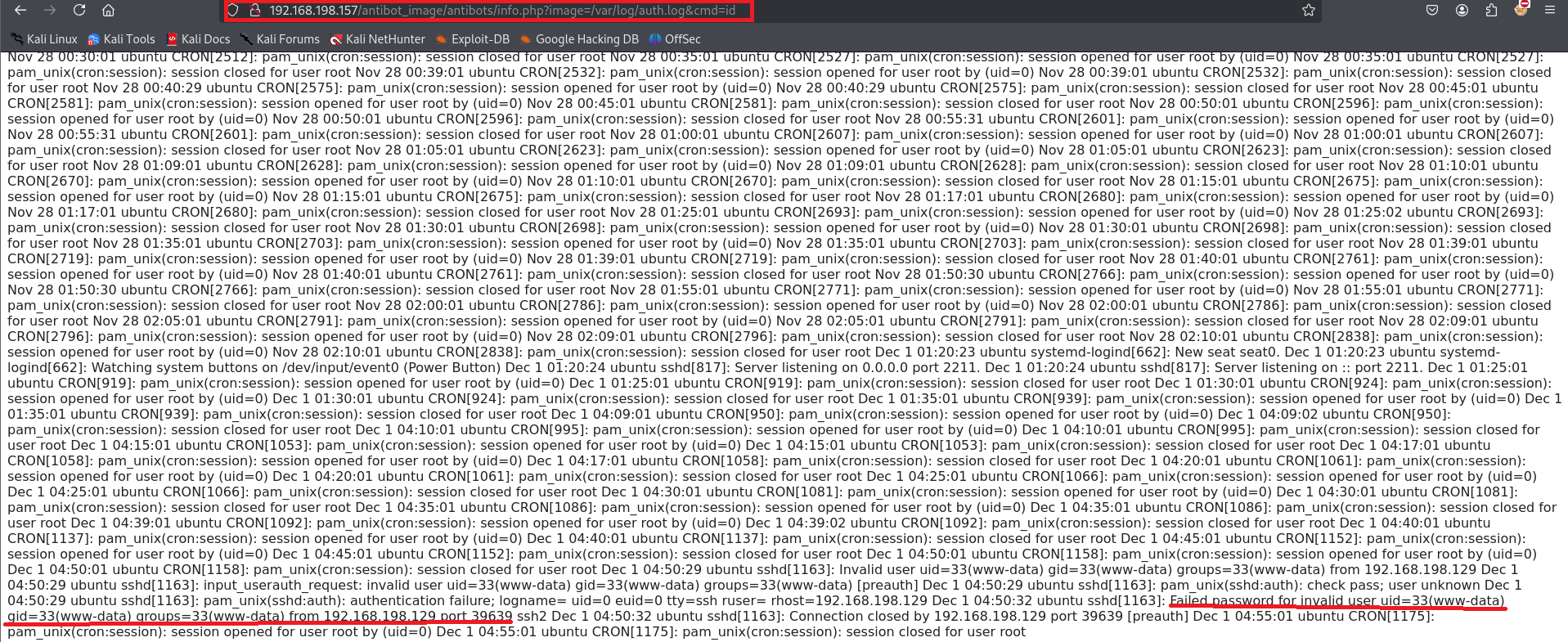


Sử dụng modun 8



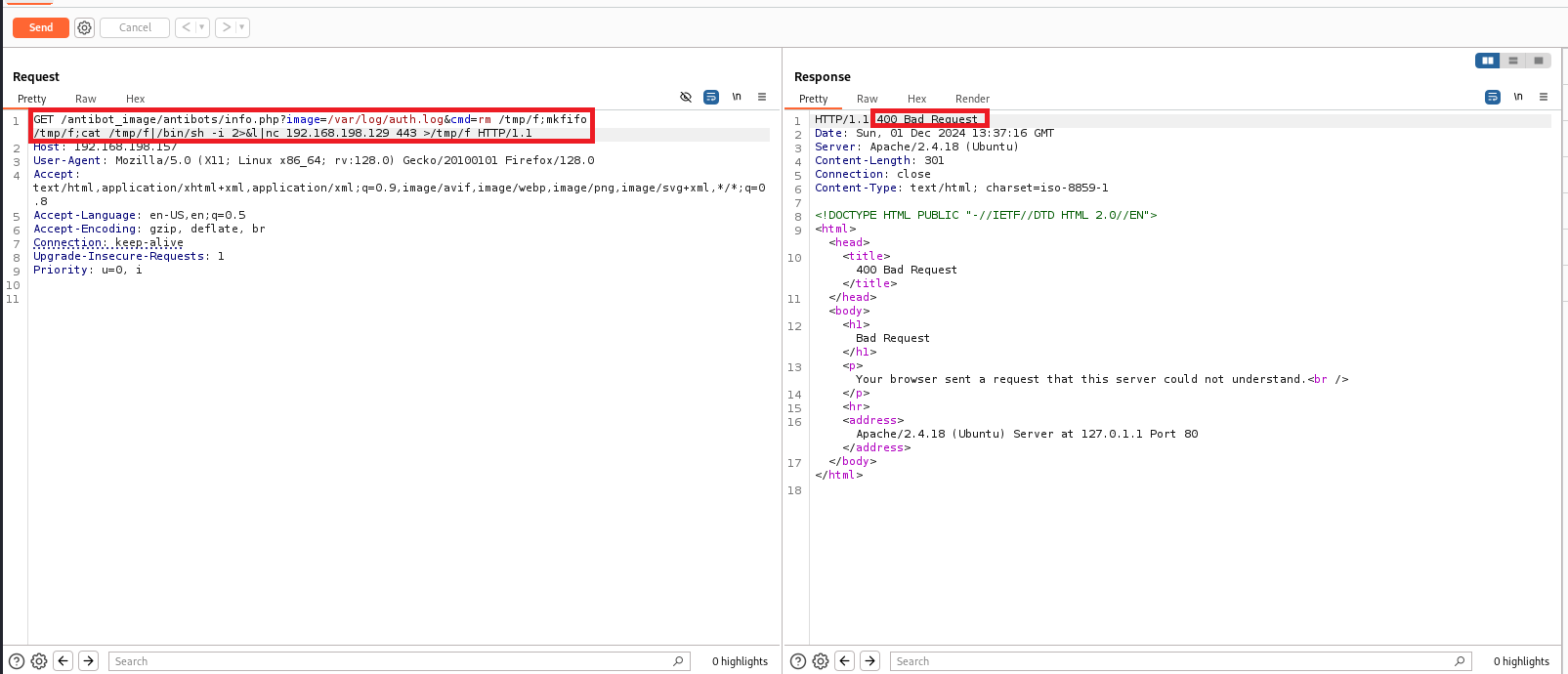


Kết quả không thành công, chúng ta sẽ quay lại trình duyệt của mình và truy cập vào tệp **/var/log/auth.log** và truyền tham số **cmd=id**

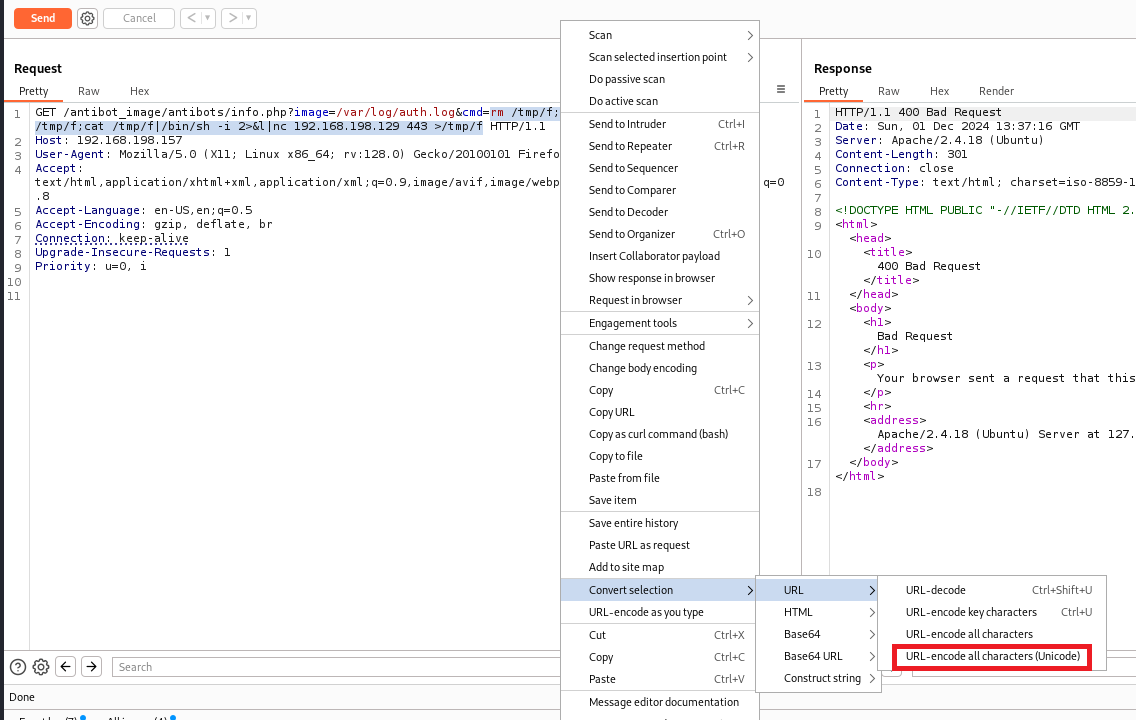


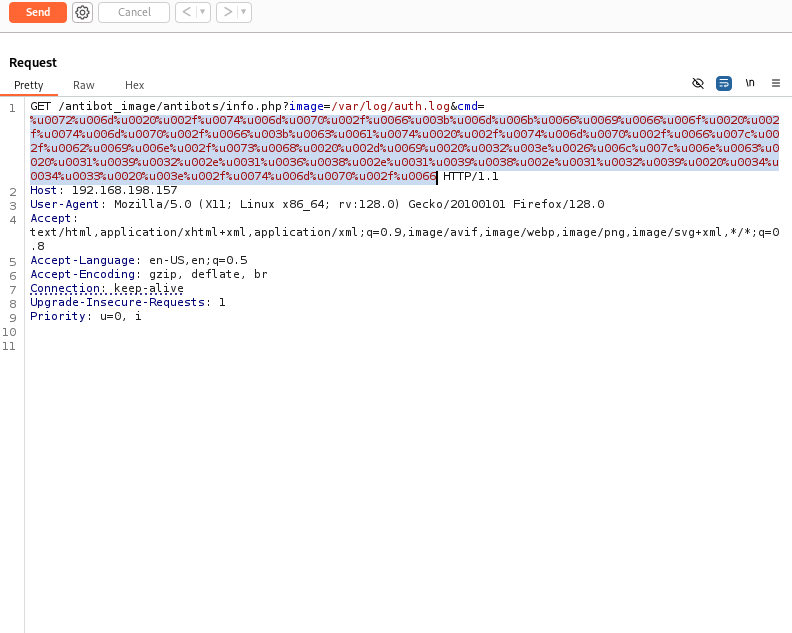
Chúng ta thấy rằng khi thực hiện lệnh, chúng ta lặp lại các bước, nhưng lần này chúng ta sẽ chèn một **reverse shell** để truy cập vào bên trong máy.

Sử dụng **BurpSuite**



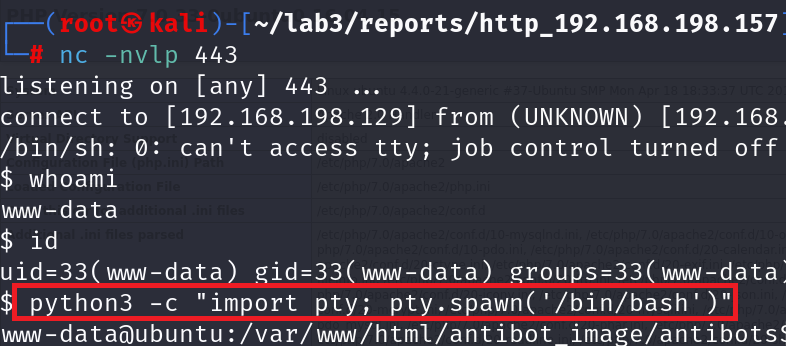
Lệnh trong “plain text” sẽ không hoạt động, do đó chúng ta phải mã hóa nó trong “**URL-encode all characters**” bằng **Burp**, như sau.



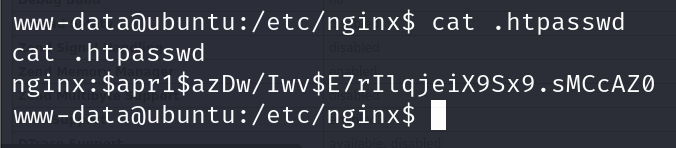


Chúng ta dùng **netcat** để lắng nghe vào cổng **443** và gửi yêu cầu từ **Burp**.

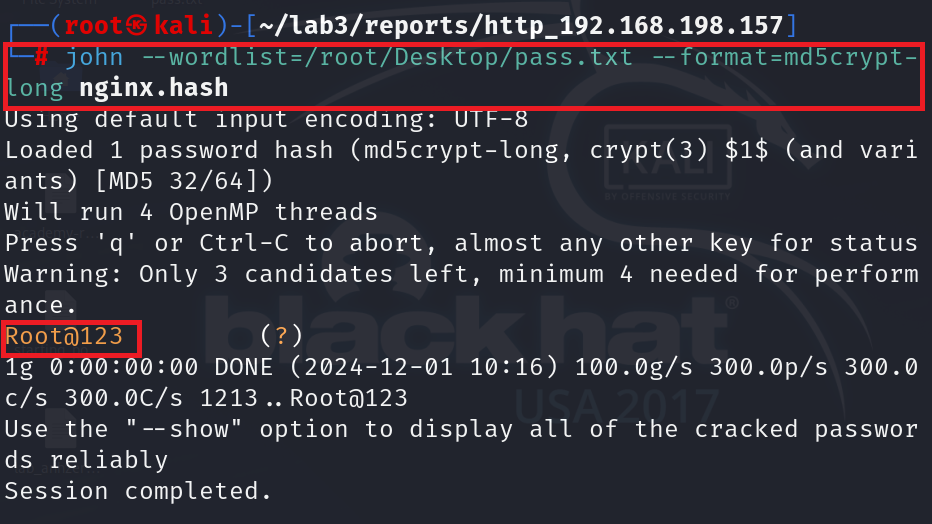
Chúng ta sẽ ở bên trong hộp, chúng ta sẽ thực hiện một vài lệnh để có một interactive shell.



Nếu chúng ta còn nhớ trước đây, trong dịch vụ **8888**, chúng ta được yêu cầu xác thực trang web bằng **.htpasswd**.

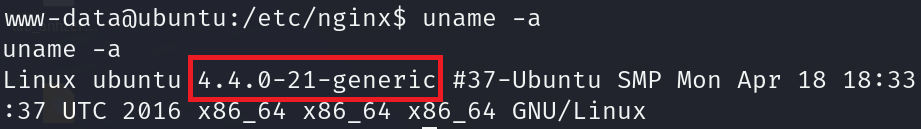


Chúng ta bẻ khóa hàm băm bằng John và từ điển kaonashi, chúng ta có được mật khẩu, nhưng mật khẩu này sẽ không hữu ích cho bất kỳ người dùng nào trong hai người.



### ****Privilege Escalation (root)****

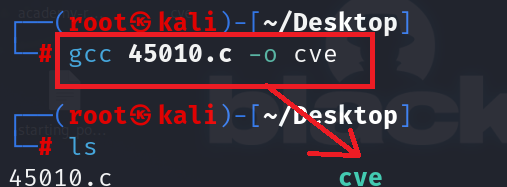
Lần này, chúng ta sẽ không thử mở rộng quy mô người dùng trước, chúng ta có lợi thế là hệ thống chưa được cập nhật và **kernel** dễ bị tấn công.

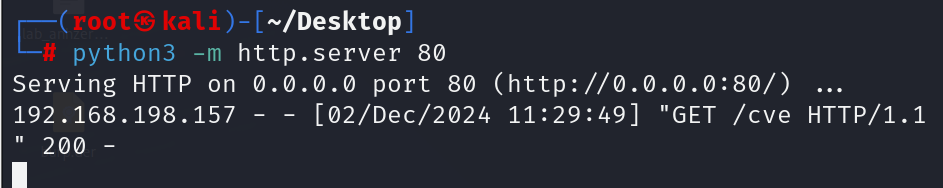


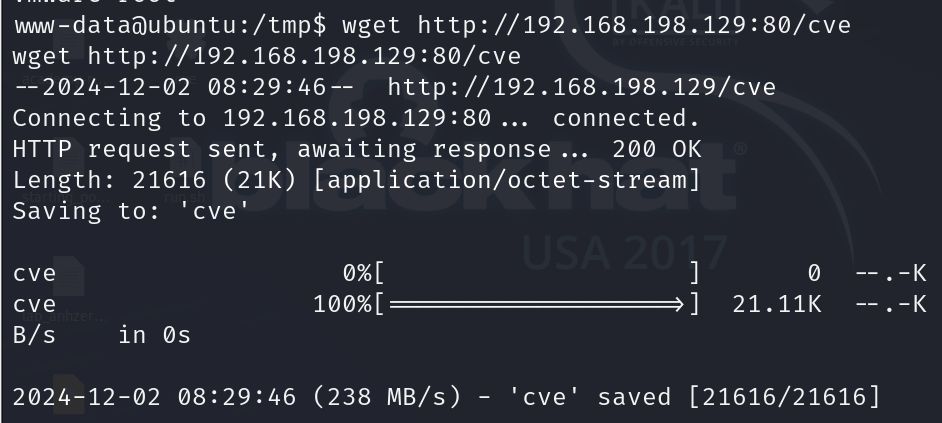
Chúng ta sẽ sử dụng khai thác sau đây để có được quyền ưu tiên như **root**.

**Exploit**: [**https://www.exploit-db.com/exploits/45010**](https://www.exploit-db.com/exploits/45010)

Chúng ta tải exploit về máy của chúng ta, biên dịch nó (*Sử dụng GCC để biên dịch file .c thành một file thực thi.)* và tải nó về máy của nạn nhân.







Bây giờ chúng ta sẽ cấp cho nó quyền thực thi và thực thi nó, điều này sẽ trả về một dấu nhắc với tư cách là root và chúng ta sẽ đọc tệp “**proof.txt**“.

