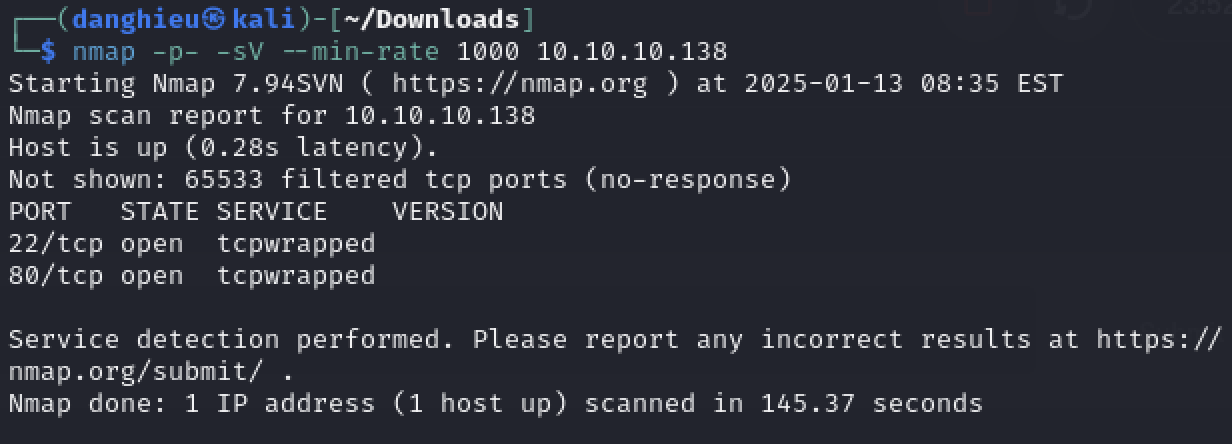
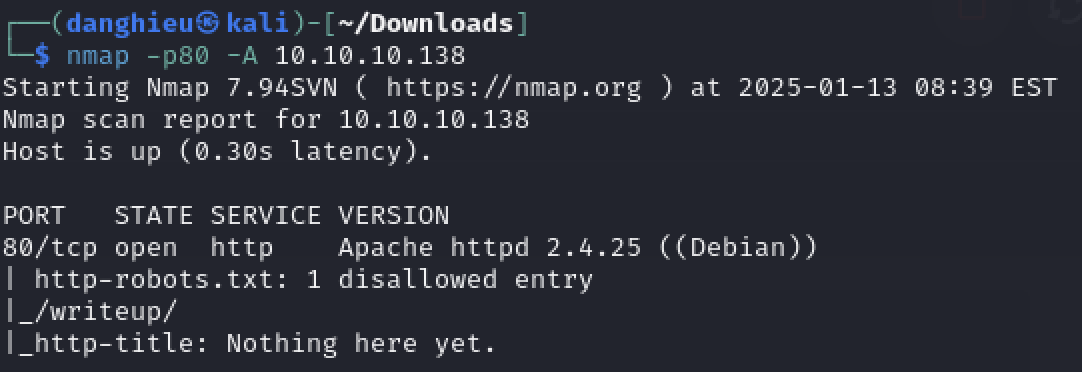
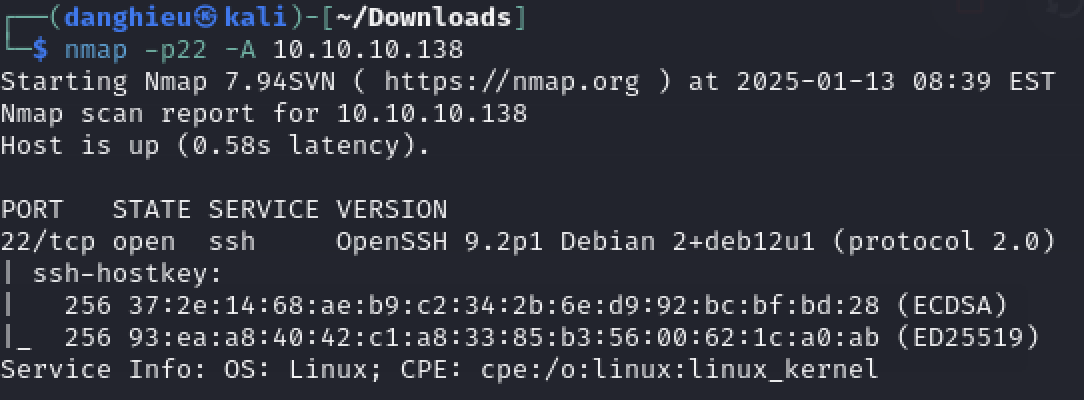
**Network**

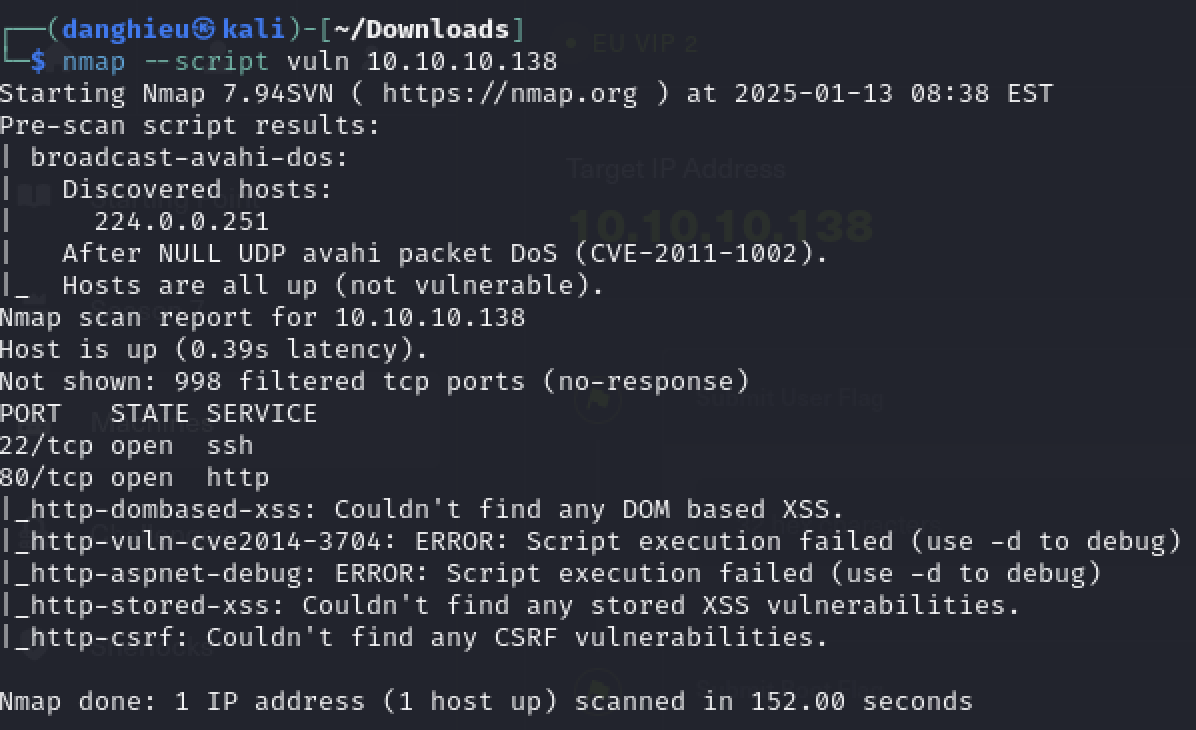


Quét như vậy mình không rõ phiên bản của dịch vụ nên mình sẽ quét chi tiết từng cổng



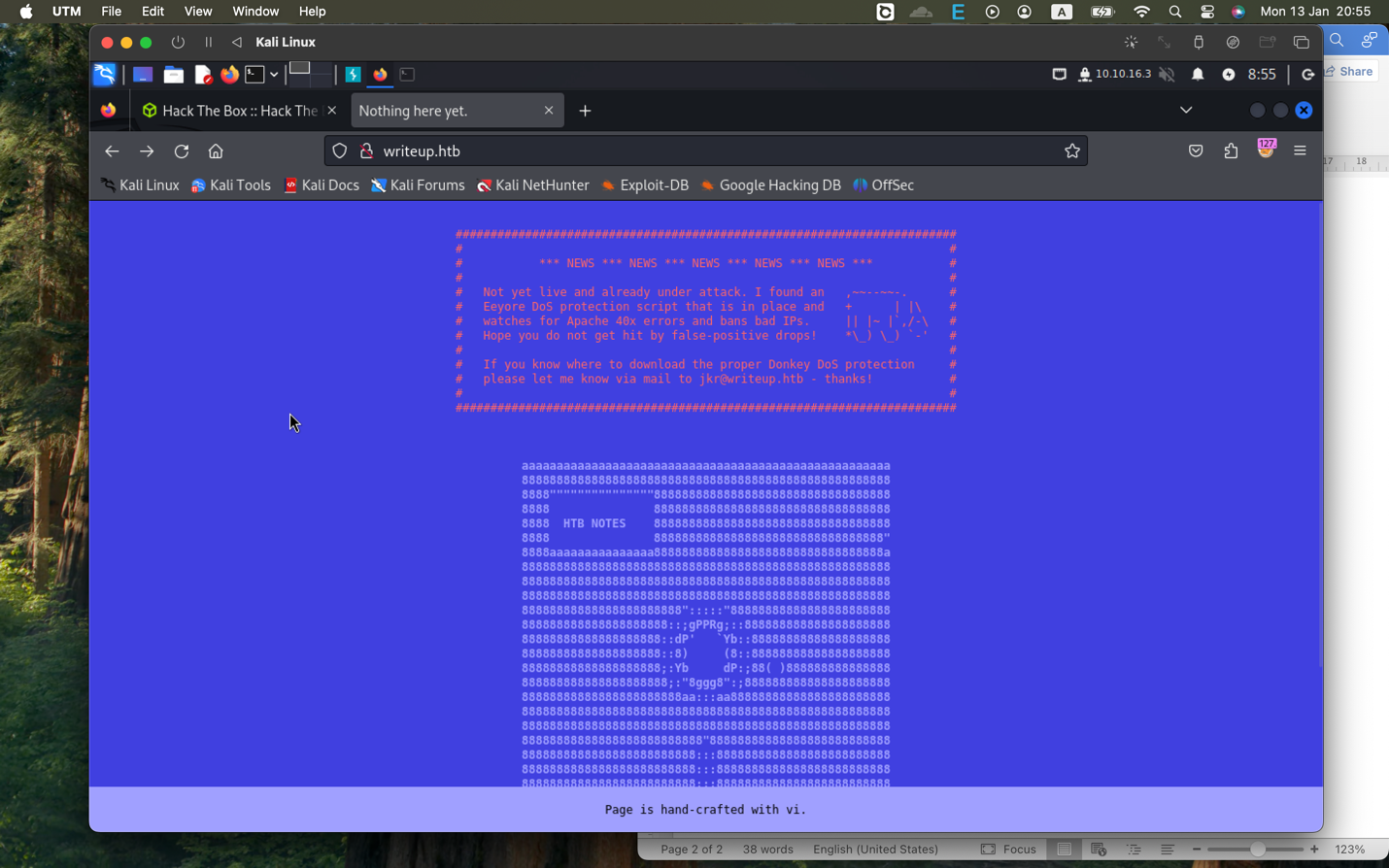


Quét lỗ hổng của dịch vụ:



**Web**

Giao diện trang web:

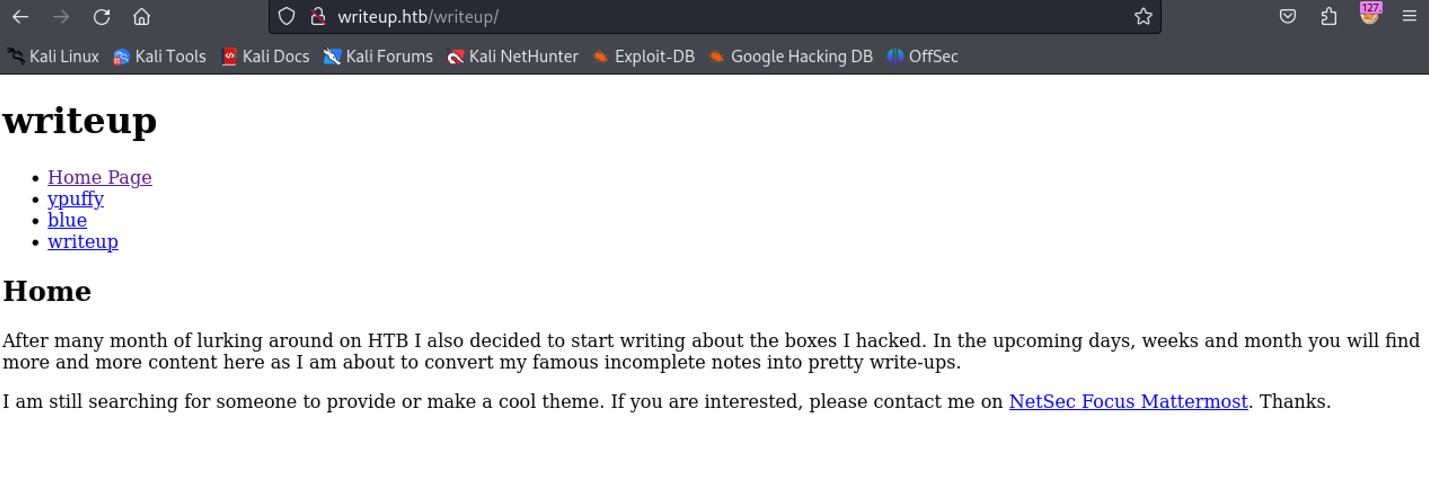


Tìm các thư mục bị ẩn

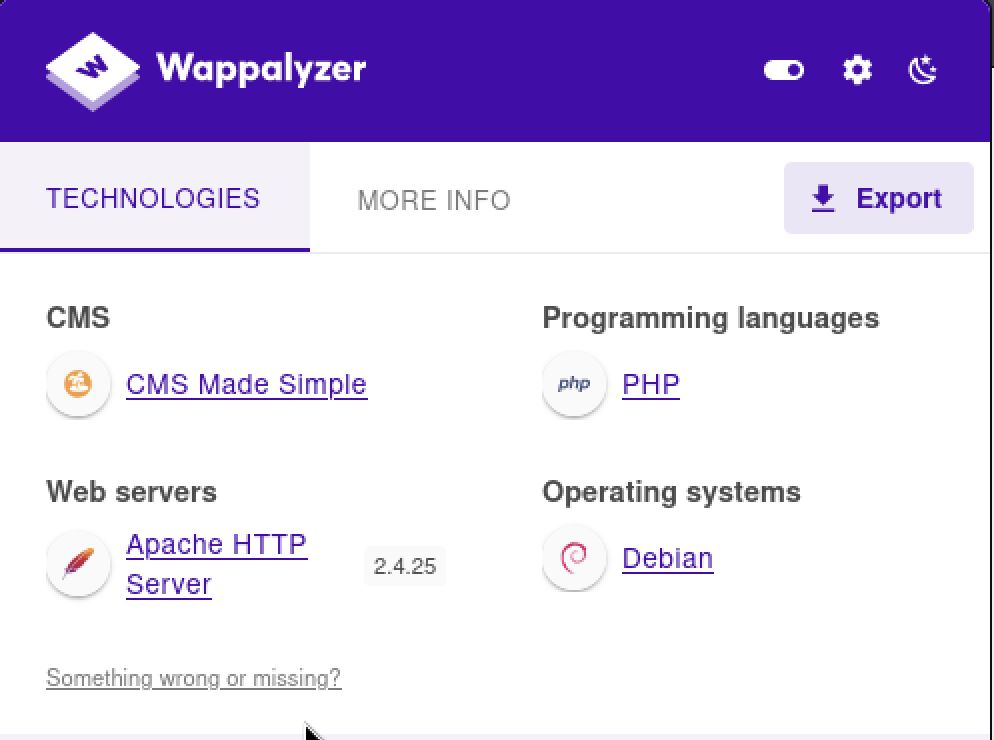
ffuf -w ./wordlists/directory-list-1.0.txt -u http://writeup.htb/FUZZ -c

Trang có tập lệnh chống DoS nên mình quét rất chậm, không tìm được thêm thư mục nào.

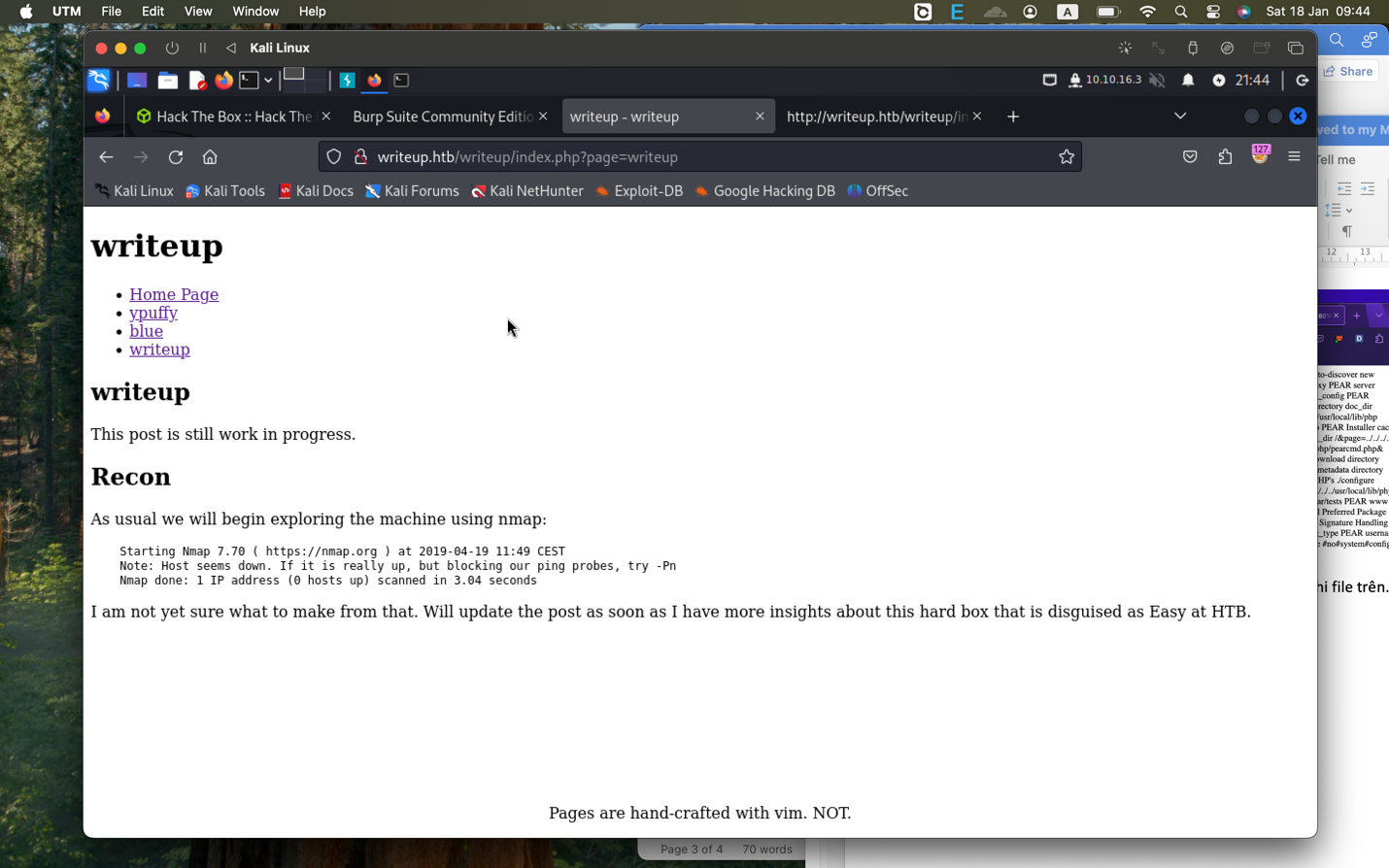
Thư mục writeup



Công nghệ trang web sử dụng:



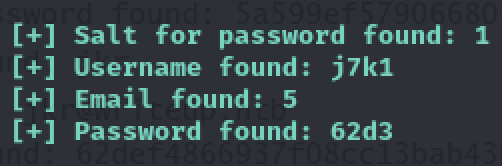
Mình kiểm soát được tham số page:



Nhưng trang web không bị dính lỗ hổng File Inclusion

Trang web dùng CMS Made Simple, mình tìm thấy 1 CVE khai thác lỗ hổng SQL Injection để trích xuất mật khẩu

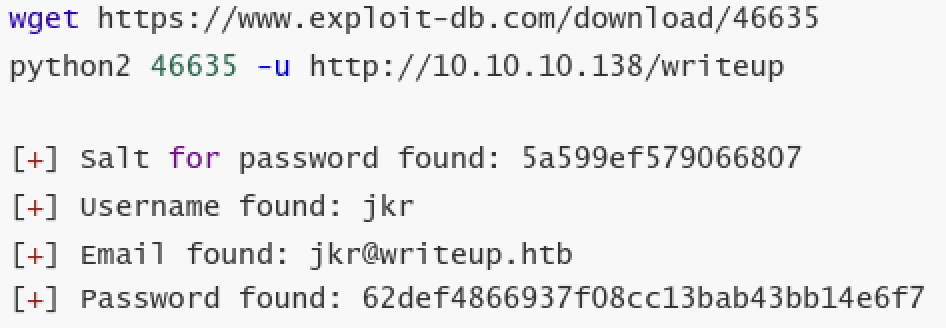
python2 46635.py --url=http://writeup.htb/writeup/



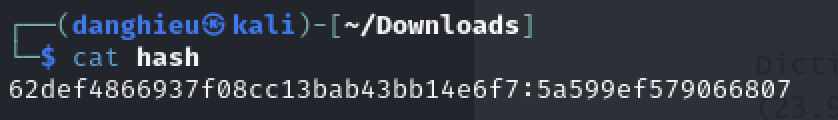
Nó tìm được hash và salt không đúng định dạng. Mình tưởng không khai thác được. Mình đi tìm nhiều cách khác. Mất rất nhiều thời gian. Không biết do lỗi của máy ảo hay chip ARM của máy.

Nếu tập lệnh ra đúng hash thì mình đã làm xong bài này lâu rồi. Nghe chán quá.

Vậy mình sẽ lấy kết quả của writeup để làm tiếp:



Sao chép hash vào 1 tập tin theo định dạng hash:salt

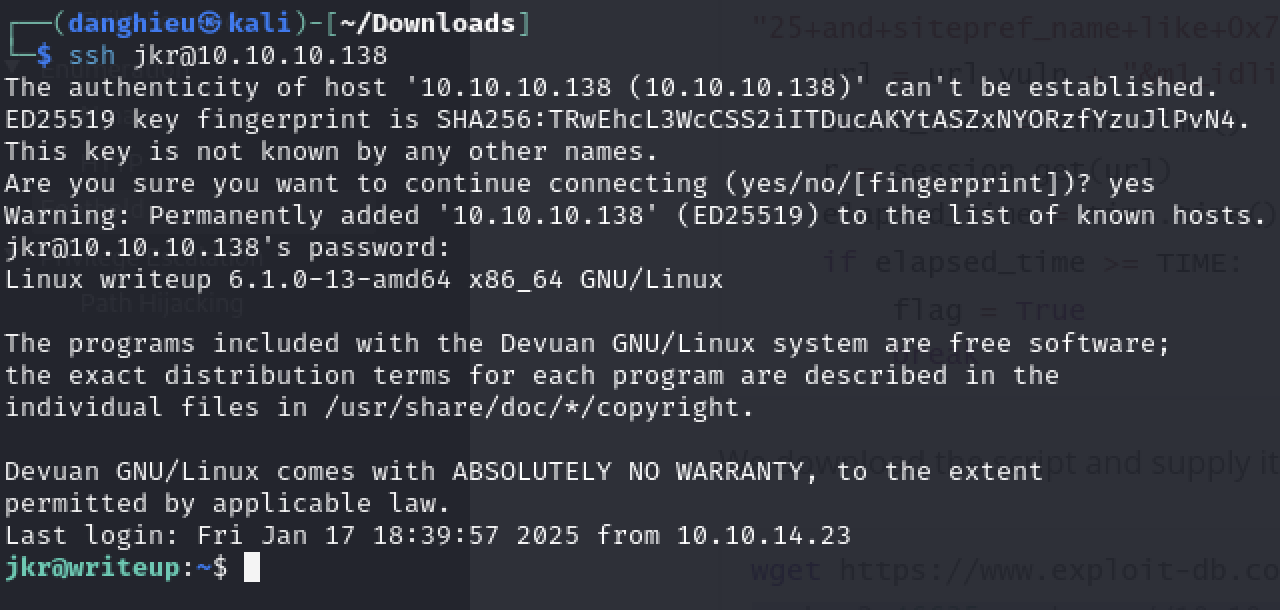


Dùng hashcat ở mode 20 để bẻ khóa hash:

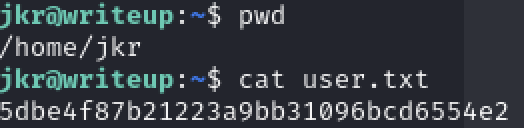


jkr : raykayjay9

Kết nối đến dịch vụ SSH:



**Privilege Escalation**





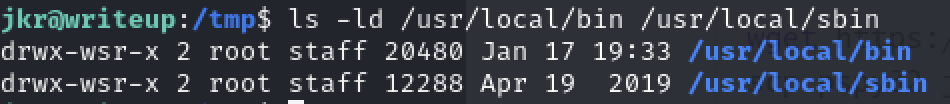
Người dùng jkr đang ở rất nhiều nhóm

Đa số là nhóm mặc định của Debian, ngoại trừ staff

Theo tài liệu của Debian:

staff: cho phép người dùng chỉnh sửa hệ thống (/usr/local) mà không cần đặc quyền của root. Người dùng nào cũng có biến môi trường là /usr/bin/local và họ có thể ghi đè các tệp thực thi trong /bin và /usr/bin

Là staff, chúng ta có thể ghi vào thư mục /usr/local/bin và /usr/local/sbin

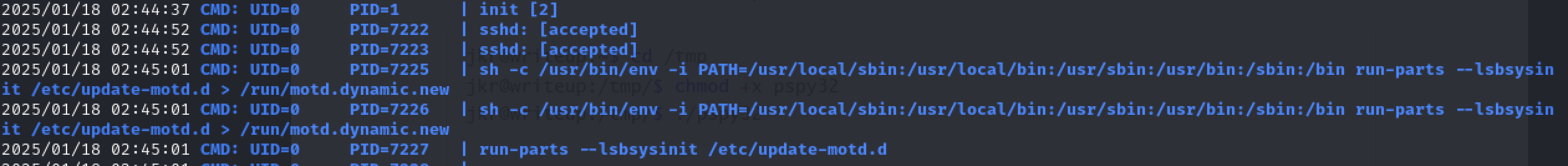


Hai đường dẫn này thường nằm trong biến môi trường PATH của root, đồng nghĩa với việc chúng ta có thể thay thế 1 chương trình mà root chạy hết những thư mục đó với 1 tập tin độc hại chứa payload cho phép chúng ta leo thang đặc quyền.

Để xem root đang làm gì trên hệ thống, chúng ta kiểm tra bằng pspy64

Chúng ta chạy tool trong 1 shell và kết nối dịch vụ SSH ở 1 shell khác

./pspy64



Khi chúng ta kết nối SSH đến máy ảo, root sử dụng tệp sh để chạy /usr/bin/env và chúng ta thấy motd được gọi. Chúng ta cũng thấy biến PATH được chỉ định trước khi chạy run-parts bao gồm 2 thư mục chúng ta có thể ghi.

Chúng ta sẽ tạo tập tin run-parts độc hại trong thư mục /usr/local/sbin, chúng ta biết nó sẽ thực thi ngay khi kết nối đến dịch vụ SSH.

Chúng ta sẽ biến tệp nhị phân bash có SUID của root, trả về 1 root shell.

echo -e '#!/bin/bash\n\nchmod u+s /bin/bash' > /usr/local/bin/run-parts; chmod +x /usr/local/bin/run-parts



Bây giờ chúng ta có thể dùng tệp nhị phân đã chỉnh sửa để lấy root shell, bằng cách dùng -p để duy trì đặc quyền

