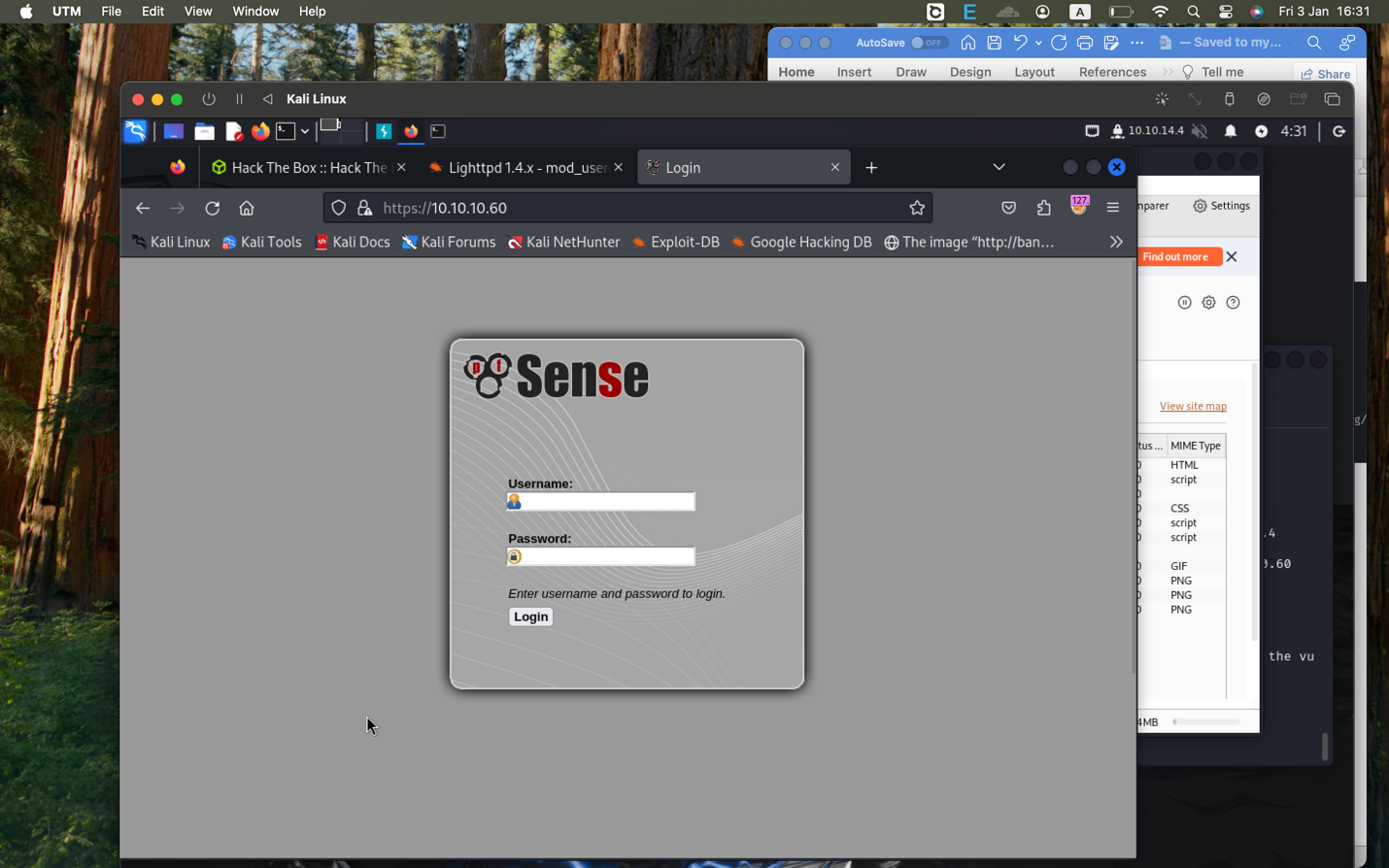


* Máy chủ web là lighttpd 1.4.35
* Ngôn ngữ server-side là PHP

Giao diện trang web



ffuf -w ./wordlists/directory-list-1.0.txt -u https://10.10.10.60/FUZZ -c

/installer/installer.php

/themes/pfsense\_ng/images/icons/favicon.ico

Khi mình tìm kiếm "sense web app exploit" thì nó hiện ra pfSense 2.3.1\_1 - Command Execution

Khai thác này yêu cầu kẻ tấn công phải xác thực

Làm sao bypass được trang đăng nhập?

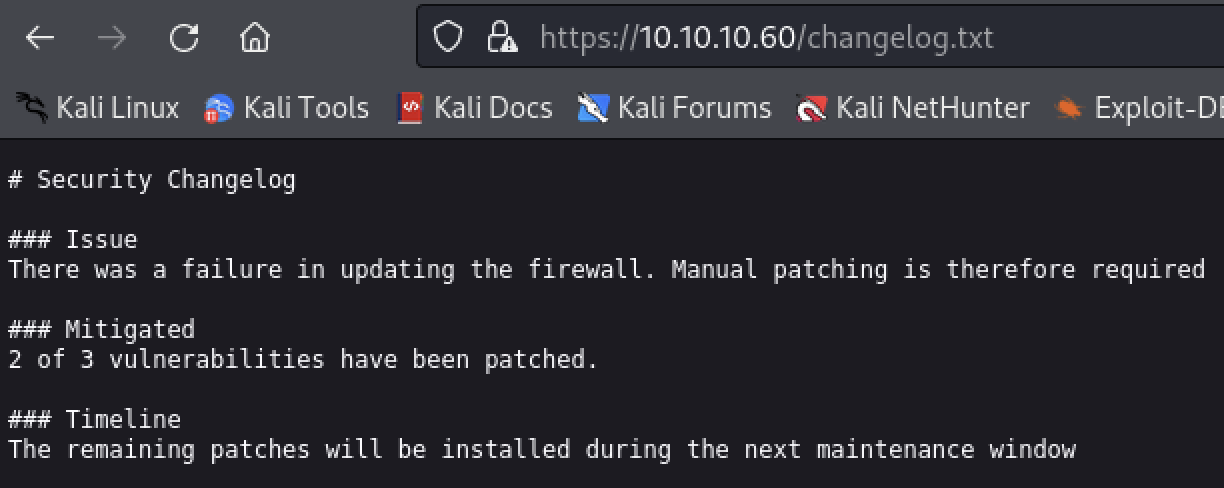
Mình có tìm tài khoản mặc định của pfsense và lighttpd nhưng đăng nhập không được

Đọc gợi ý từ hackthebox thì có 1 tập tin văn bản (.txt) chứa tài khoản của người dùng.

Mình tiếp tục tìm các thư mục bị ẩn bằng ffuf

ffuf -w ./wordlists/common.txt -u https://10.10.10.60/FUZZ -c -e .txt

Tìm được tập tin changelog.txt, nội dung khá thú vị



🡪 Rõ ràng tường lửa pfsense bị dính lỗ hổng

Liệt kê cấp 1 không được, mình tiếp tục liệt kê cấp 2, thấy có 2 thư mục đáng nghi ngờ là /includes và /installer

🡪 Không tìm thêm được file .txt

Lần này mình dùng 1 wordlist lớn hơn directory-list-2.3-medium.txt

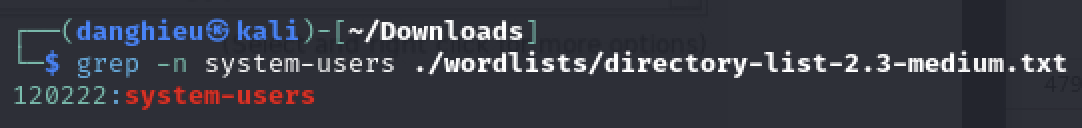
Trời ơi scan mãi không tìm được tệp văn bản nào ☺

Không biết mình dùng ffuf có bỏ qua trường quan trọng nào không

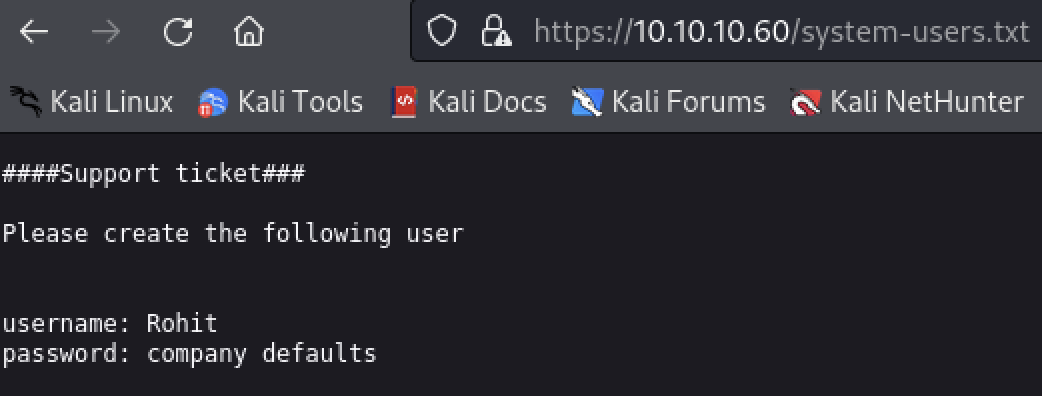
Đúng như mình nghĩ, điểm yếu của ffuf là không hỗ trợ quét đệ qui

Khi mình quét cấp 2 thư mục /installer thì wordlist common.txt lại không có system-users

Tệp system-users.txt ở trong wordlist directory-list-2.3-medium.txt nhưng lại ở vị trí khá xa



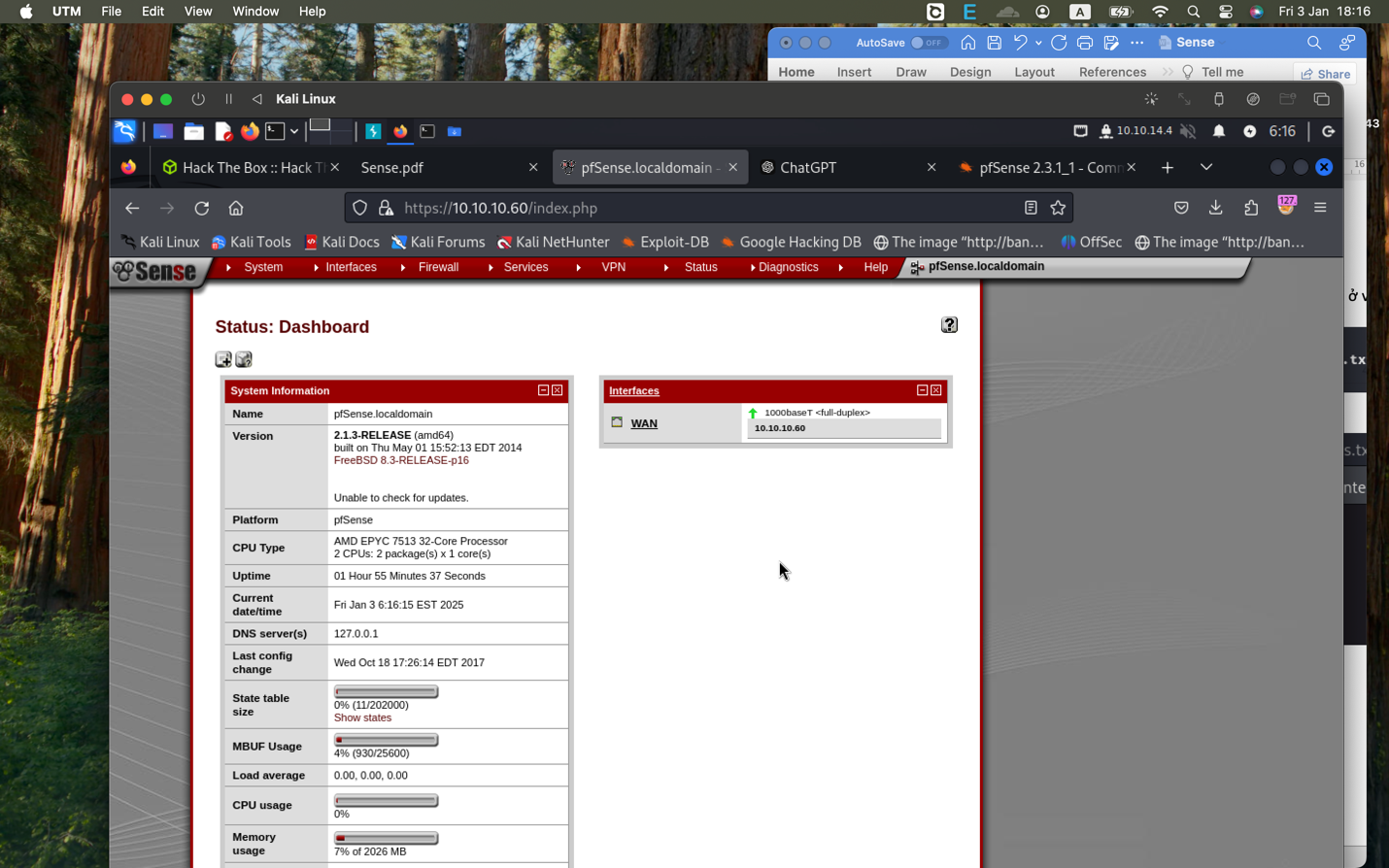
🡪 Tóm lại, bài này tìm thư mục ẩn là 1 thử thách quá lớn



Trời ơi nhập đúng thông tin trên nhưng không đăng nhập được ☺

rohit:pfsense

Giao diện trang web



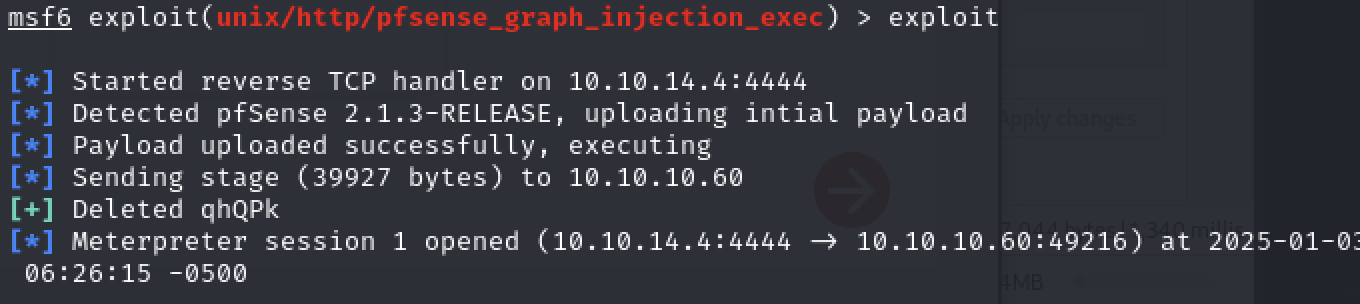
Mình không dùng được khai thác trên pfSense 2.3.1\_1 vì nó không có tính năng quản lý người dùng

Tìm kiếm 1 CVE khác tương ứng với phiên bản pfSense 2.1.3

pfSense < 2.1.4 - 'status\_rrd\_graph\_img.php' Command Injection

Đã thử trên FreeBSD 8.3-RELEASE-p16

Trên metasploit có 1 module khai thác tương tự: exploit/unix/http/pfsense\_graph\_injection\_exec



Mới gaining access mà đã được root rồi thì …

