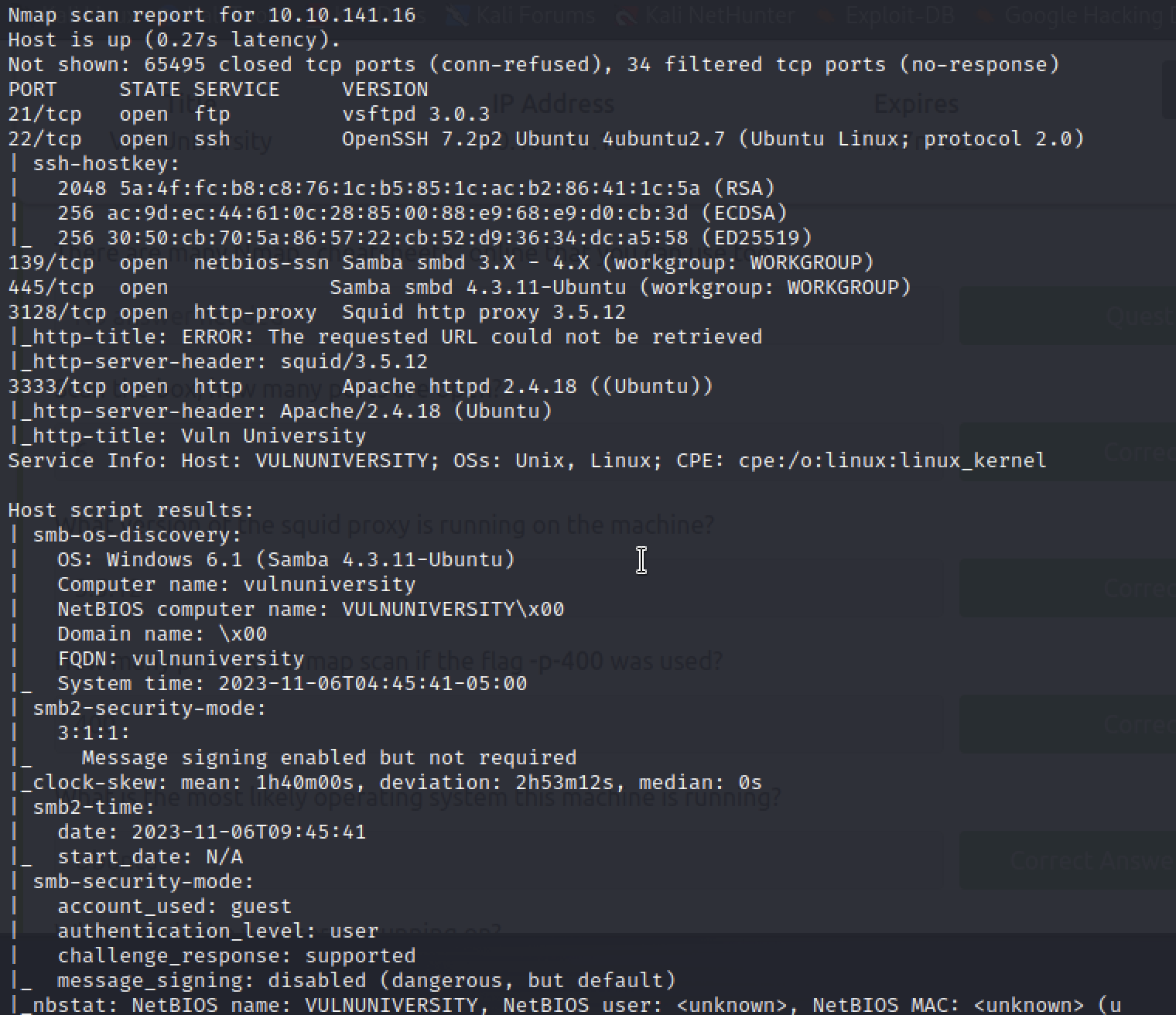
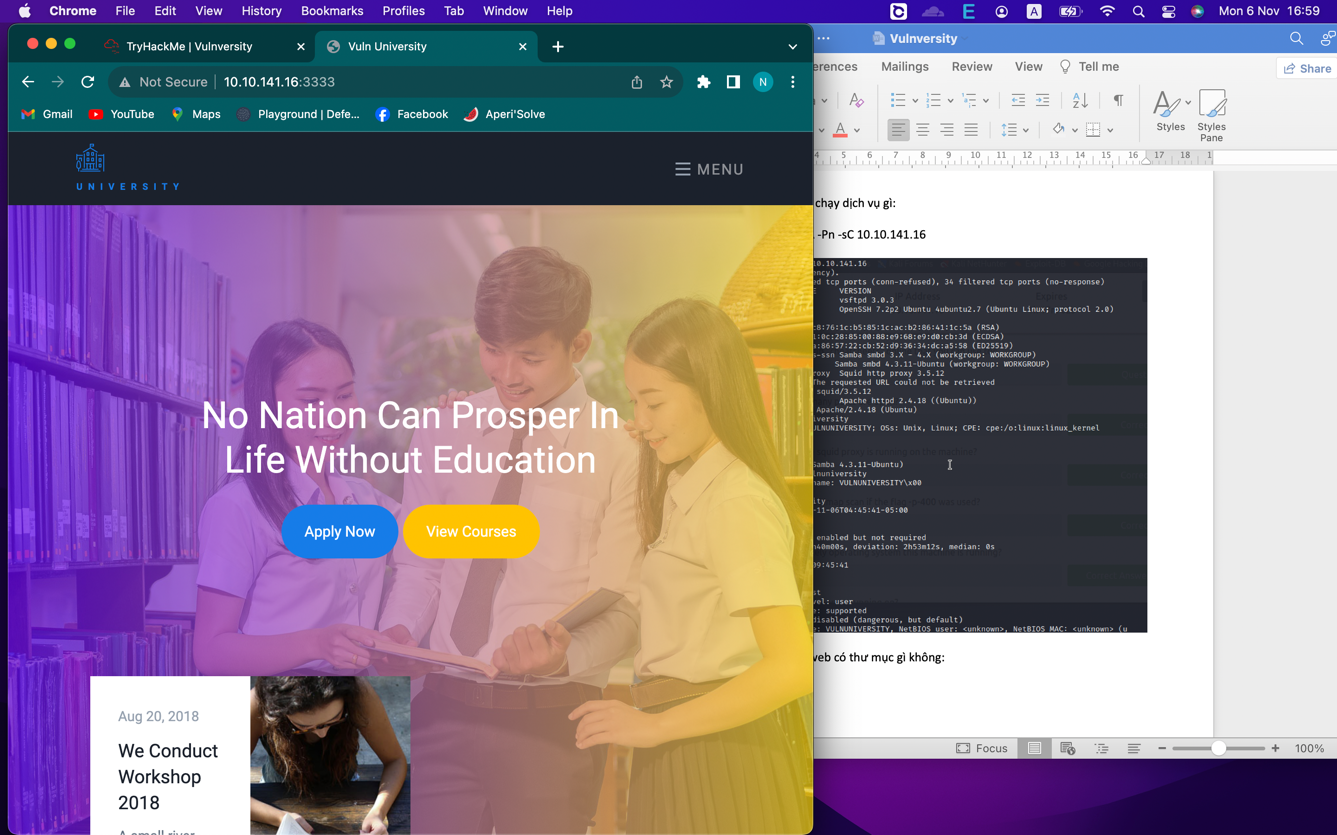
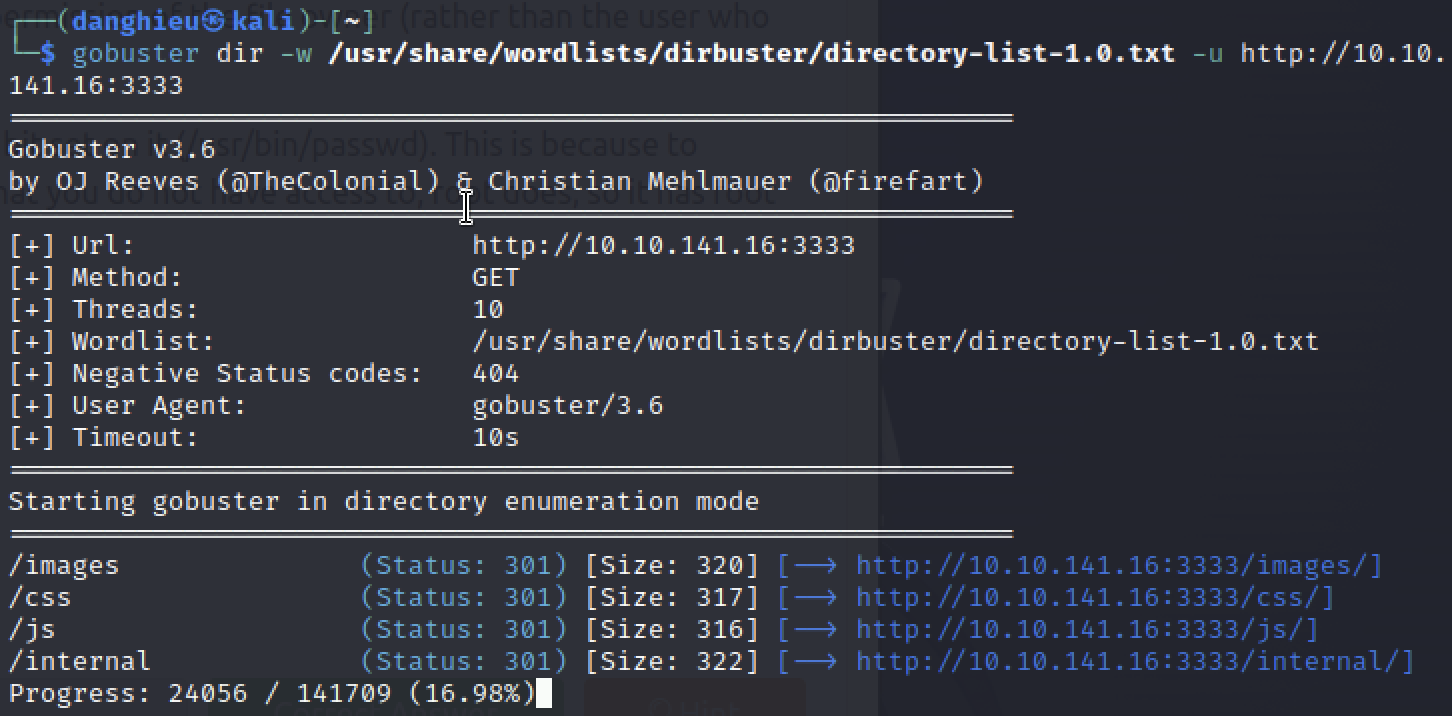
Quét xem máy chủ chạy dịch vụ gì:

nmap -sV -p- -T4 -A -Pn -sC 10.10.141.16





Quét xem dịch vụ web có thư mục gì không:

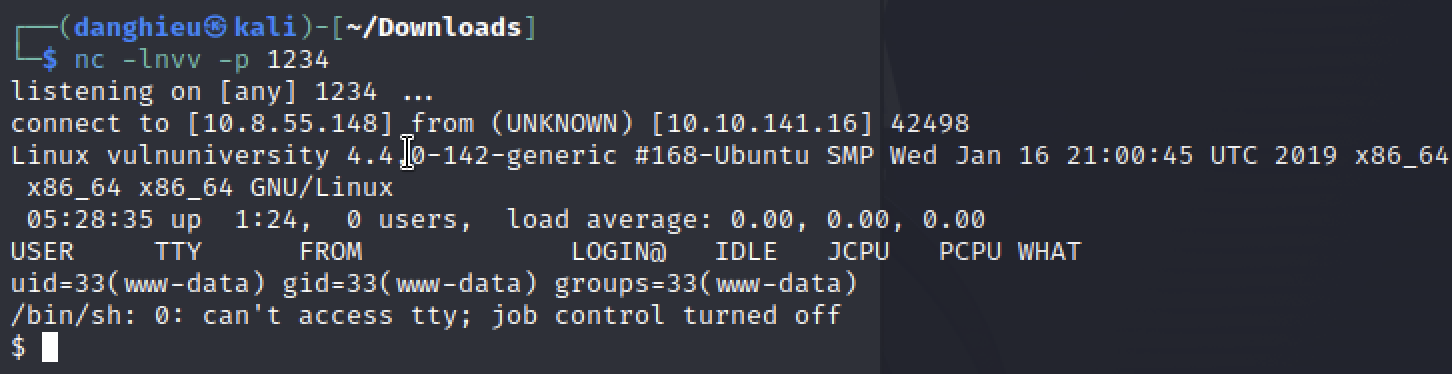


* Thư mục images
* Thư mục internal cho bạn upload file

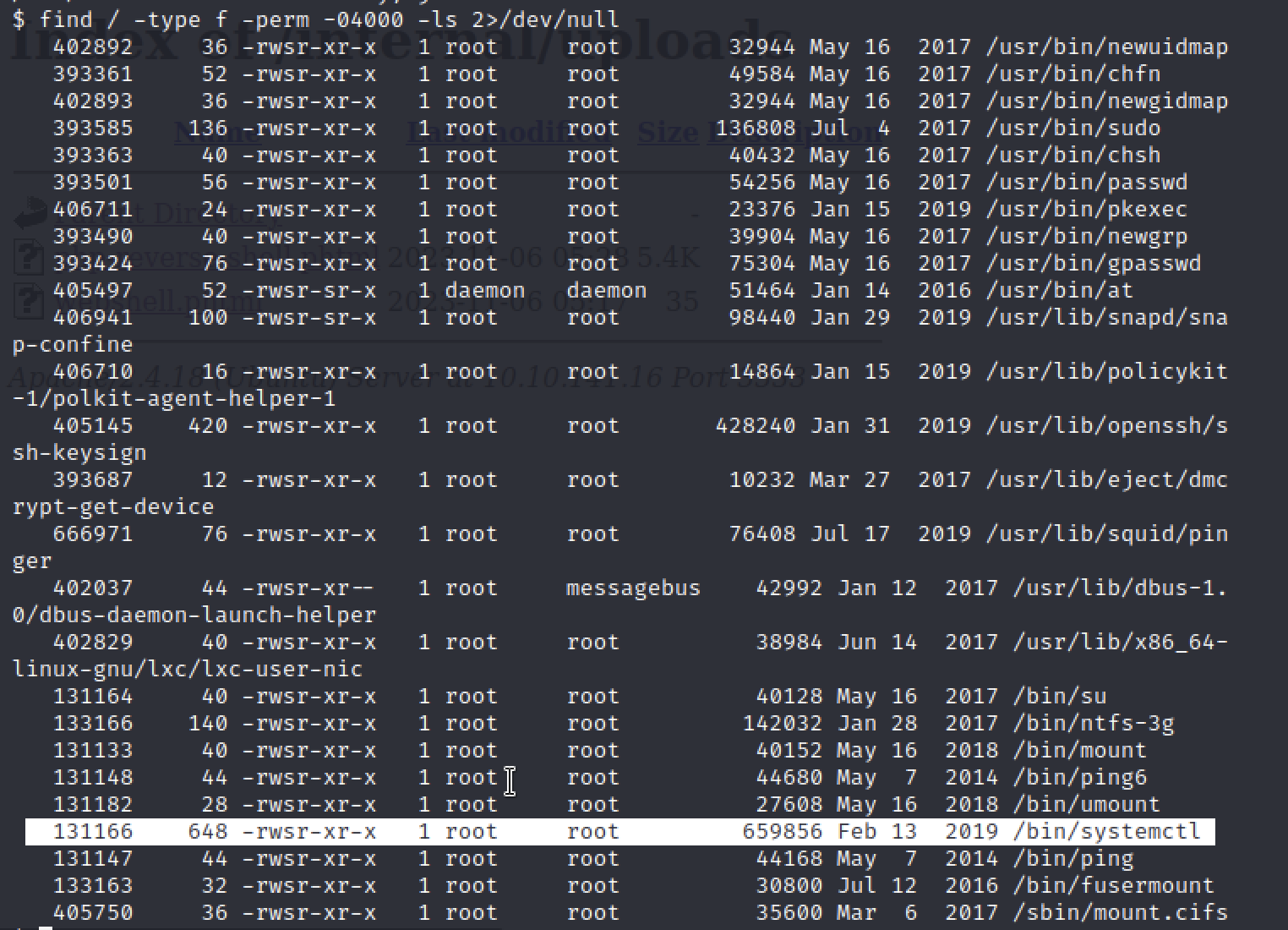
Bài này hơi xàm. Chức năng upload file không cho up file .jpg, .jpeg. Thêm nữa không cho mình biết đường dẫn để đọc file. Nó không giống với web ctf. Buộc mình phải làm theo hướng dẫn.

* Up 1 file php-reverse-shell.phtml lên trang internal (thay đổi ip, port)
* Đọc file ở http://10.10.141.16:3333/internal/uploads/php-reverse-shell.phtml

Bạn sẽ có được reverse shell:



Để leo thang đặc quyền, tìm file có SUID:



Ở đây, có systemctl là dùng được. Bạn không thể có shell ngay lập tức nhưng đọc được file hệ thống

File bạn muốn đọc là /root/root.txt

