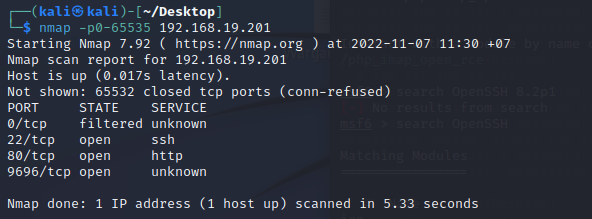
Flag 01



Ảnh có chứa văn bản

Mô tả được tạo tự độngẢnh có chứa văn bản

Mô tả được tạo tự động

Flag03



* Khi dùng burp site để xem request thì ta thấy có 1 host lạ là [www.alunno.inseclab](http://www.alunno.inseclab)

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

* Khi truy cập thì trình duyệt lại không tìm thấy hosts
* Sau khi tìm hiểu thì thấy để có thể truy cập váo thì ta phải thêm địa chỉ ip cũng như tên hosts vào /etc/hosts

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

* Sau đó đăng nhập lại thì ta được trang như trên

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi dùng dirbsearch thì ta thấy có 1 directory khả nghi là /admin nên truy cập vào thử

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, đen

Mô tả được tạo tự động

* Ta thấy được 1 trang web django admin yêu cầu email và passs
* Nhưng khi dùng email và pass đã đăng ký ở trang chính thì lại không được nên sau khi tìm ở trang github của tác giả thì ta thấy có database của trang web

Ảnh có chứa văn bản

Mô tả được tạo tự động

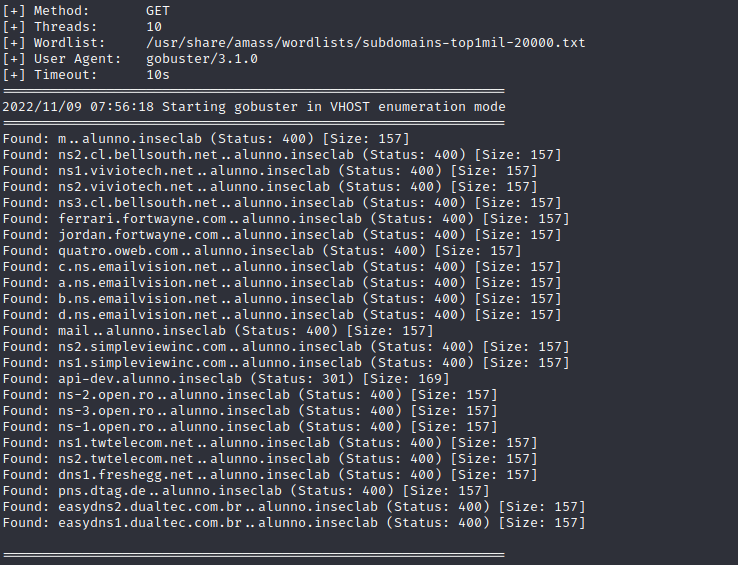
* Và email cũng như pass của super user là admin

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy có member là flag và truy cập vào thì thấy flag03

Flag02



* Sau khi quét tìm VHOSTS ta thấy có 1 hosts là api-dev.alunno.inseclab và cũng không truy cập được như ở trên nên ta thêm vào /etc/hosts

Ảnh có chứa văn bản

Mô tả được tạo tự động

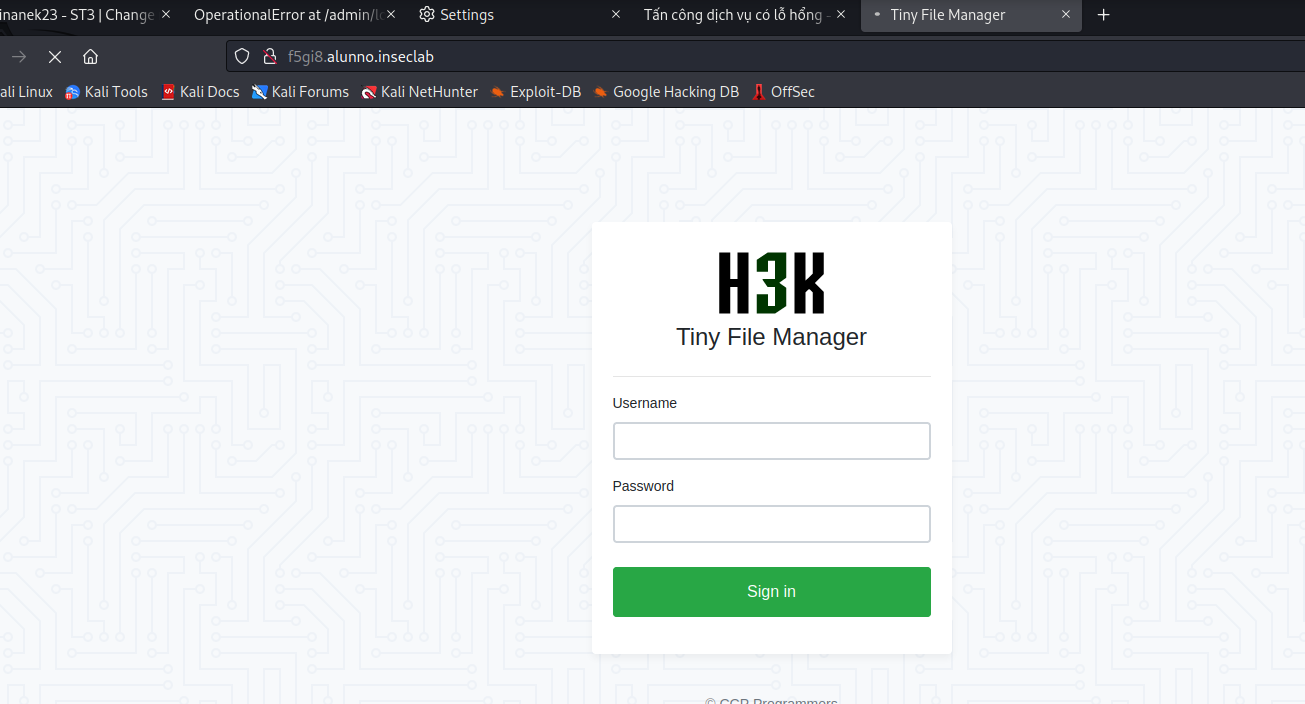
* Sau khi truy cập thì ta thấy flag02

Flag04

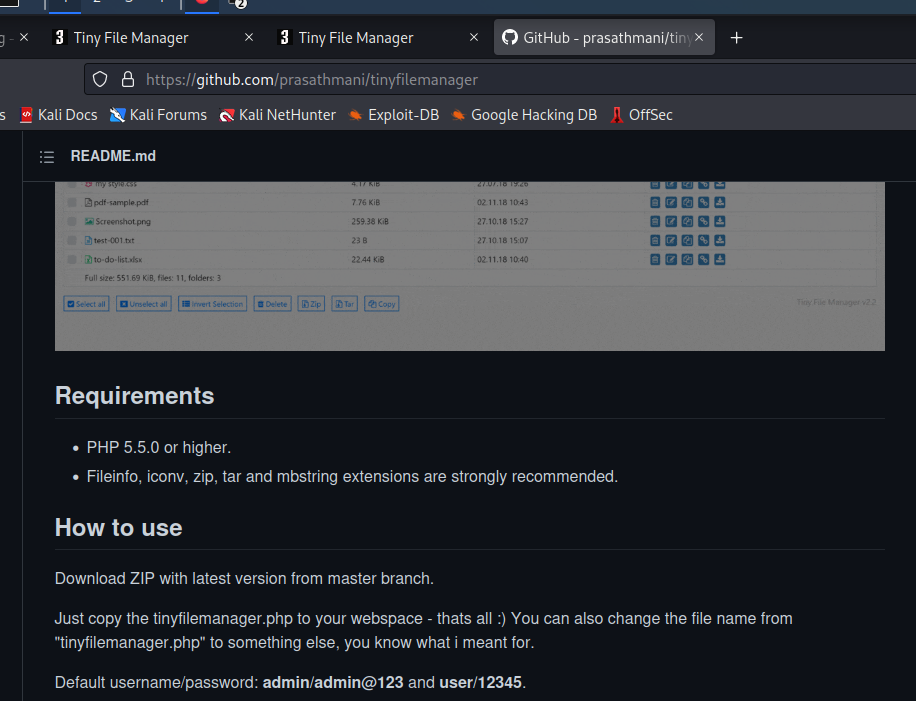
Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, đen

Mô tả được tạo tự động

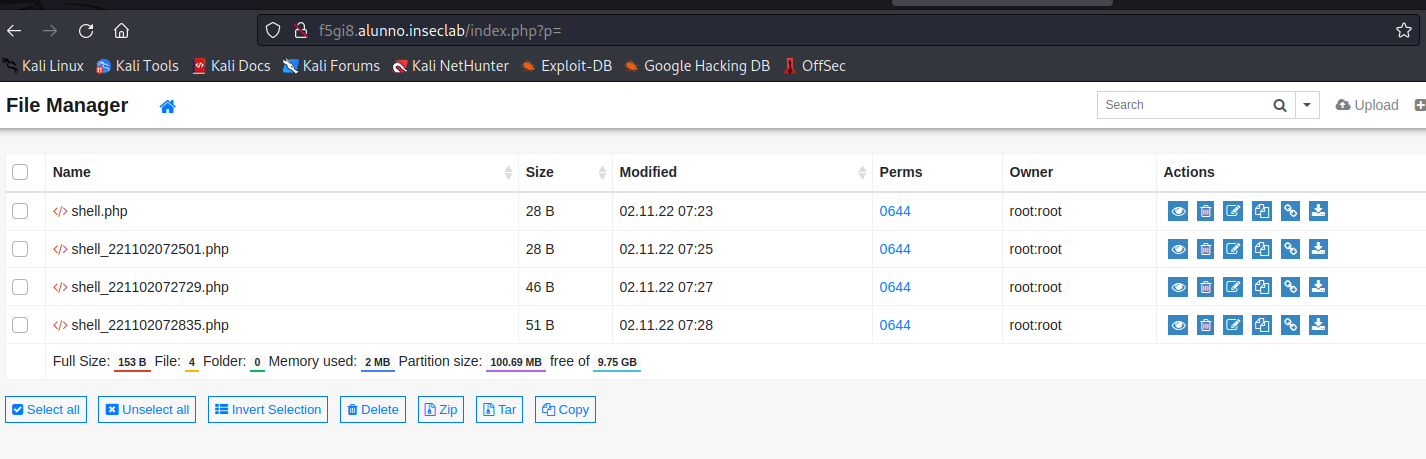
* Sau khi vào trang admin của api-dev thì ta thấy có 1 lesson tên là Tấn công dịch vụ có lỗ hổng và có 1 đường link



* Nó cũng phải thêm vào /etc/hosts để có thể truy cập và ta được trang như trên



* Sau khi truy cập trang của tác giả thì ta thấy pass và username dùng để đăng nhập



* Ta xem từng file

Ảnh có chứa văn bản

Mô tả được tạo tự động

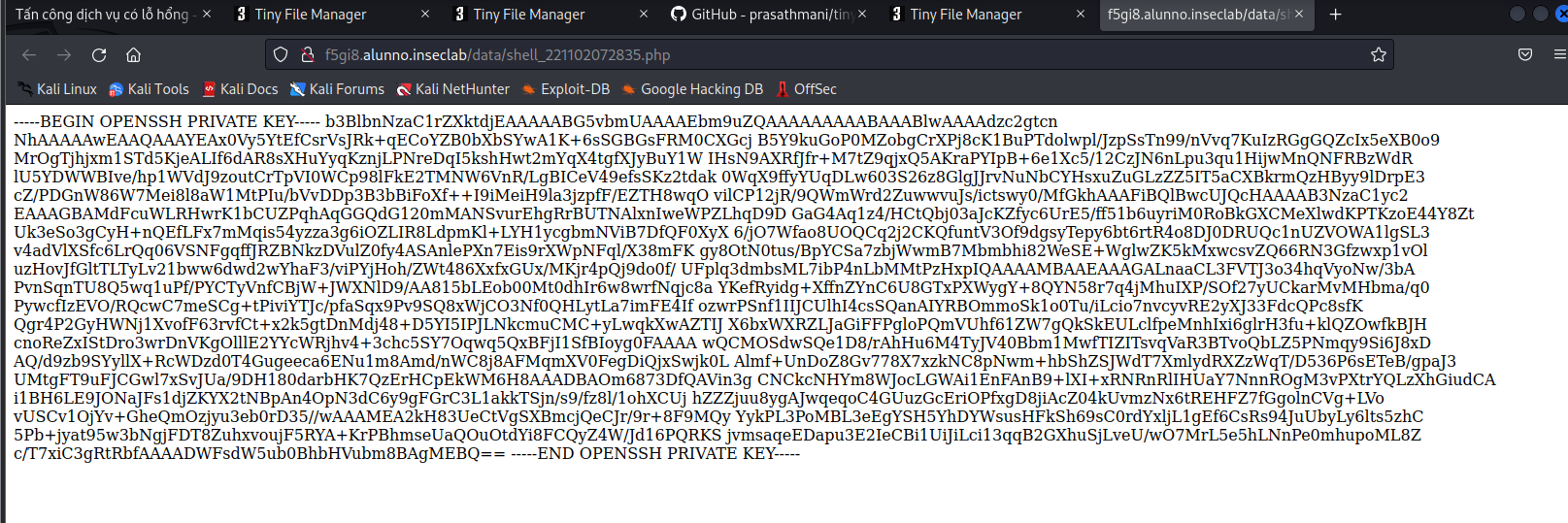
* File này có tạo command mở 1 file flag ta truy cập thử

Ảnh có chứa văn bản

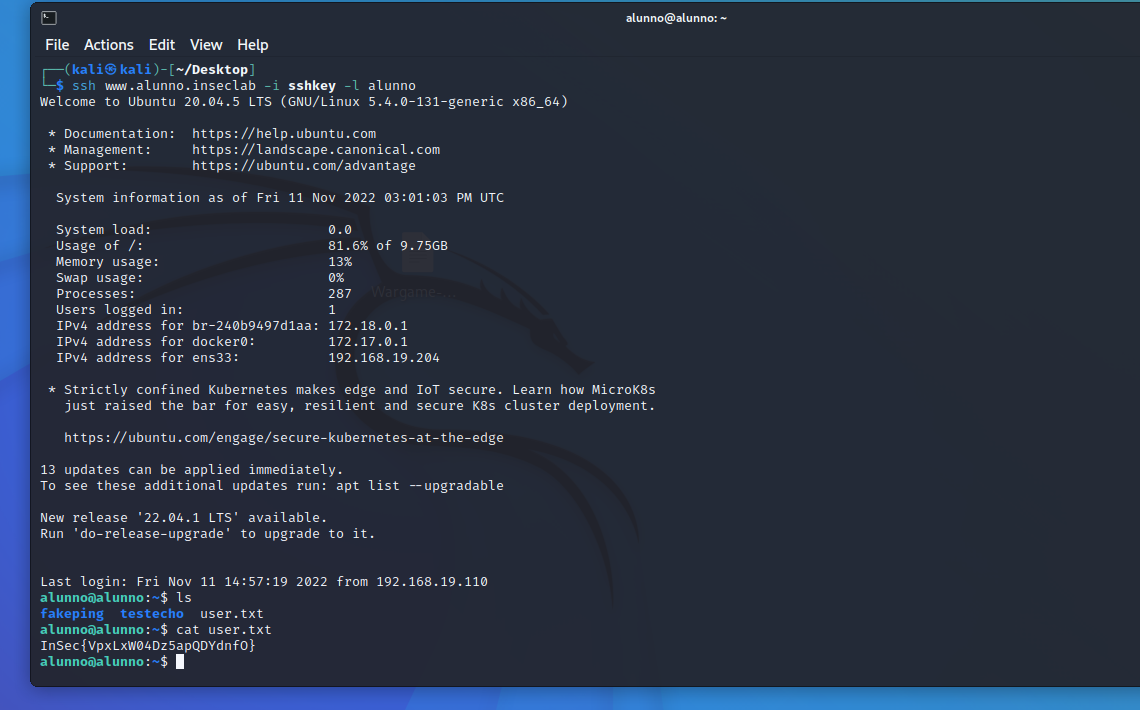
Mô tả được tạo tự động

* Ta thấy flag04

Alunno User



* Trong các file ta thấy có file key dùng để xác thực kết nối ssh



* Dùng ssh key để xác thực và với user là alunno
* Ta dùng lệnh ls xem các file và thấy có file user.txt và có flag cho user alunno

Flag05



* Ta xem thử các thư mục có thể vào trong máy thì thấy có 1 file lạ tên là u7wq và đọc thử

Ảnh có chứa văn bản

Mô tả được tạo tự động

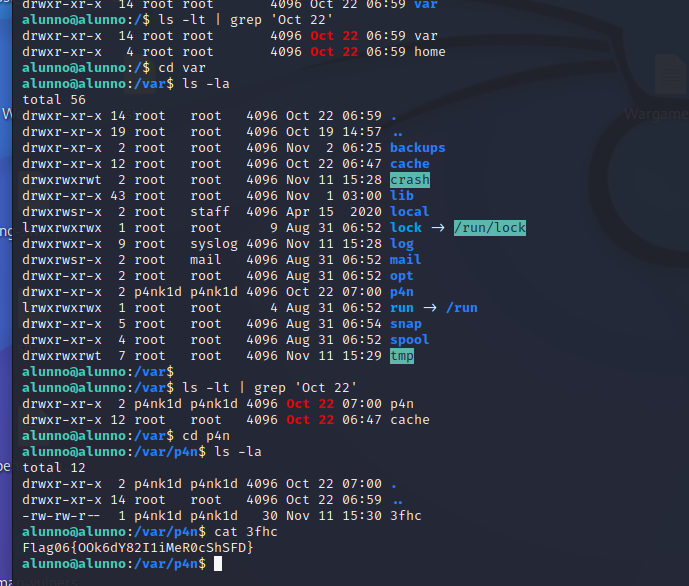
* Trong có có flag05

Flag06

Ảnh có chứa văn bản

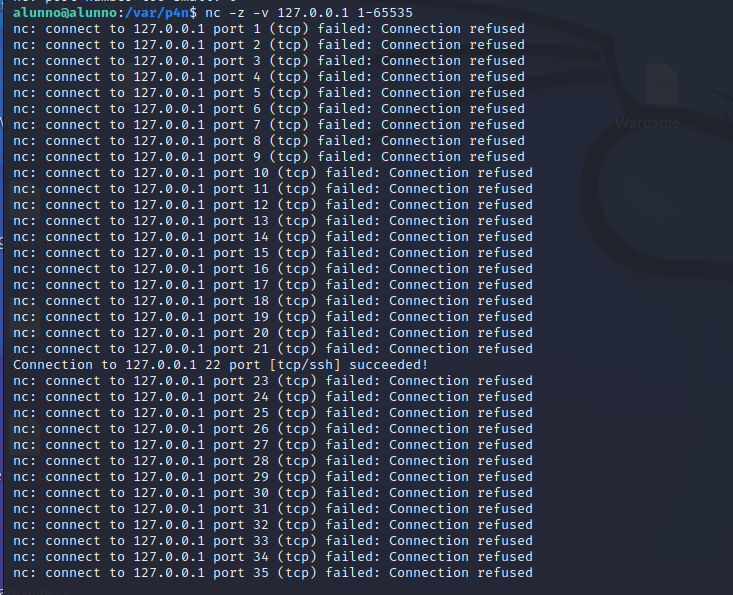
Mô tả được tạo tự động

* Từ lệnh ls ta có thể thấy file user.txt được tạo 28 Oct ta kiếm những file có cùng ngày tạo xem sao



* Ta chạy lệnh ls -lt | grep 'Oct 22'
* Sau đó vào folder var và cũng dùng lệnh tương tự và tiếp tục với p4n
* Sau đó thấy file 3fhc không phải là folder và cat thử thì ra flag06

Flag07



* Dùng lệnh nc -z -v 127.0.0.1 1-65535 để quét và kết nối vào các port đang mở thì ta thấy có 2 port lạ



* Port 9696 và 9697

Ảnh có chứa văn bản

Mô tả được tạo tự động

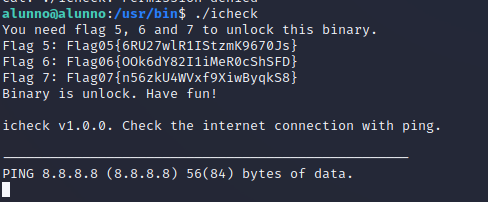
* Kết nối vào port 9696 thì sai host nên kết nối vào thử port 9697 thì ra flag07

Root Flag

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Kiếm các file có cùng ngày 22 Oct có file tên icheck và được cấp quyền để thực thi
* Ta thử thực thi file



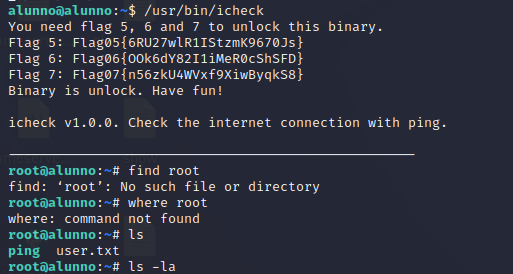
* Nó yêu cầu flag 5 6 7 và khi nhập xong thì sẽ có lệnh ping 8.8.8.8 sau đó thoát



* Ta sẽ echo “/bin/bash” vào ping và cấp quyền cho nó



* Thay đổi biến môi trường
* 
* Biến PATH mới sẽ được mở rộng để ta có thể thực thi file ping ở ngoài /home/alunno



* Ta thực thi lại file icheck và đã thành công lên root user

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Dùng lệnh file để tìm các file root và ta tìm được flag root