

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO THỰC HÀNH

**TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG**

**Bài thực hành số 1:**

**DÒ QUÉT LỖ HỔNG VÀ**

**KHAI THÁC MỘT SỐ LỖ HỔNG PHỔ BIẾN**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

**Lớp:** AT17G

**Thời gian nộp bài:** 8/12/2023

***Giảng viên hướng dẫn****:* Phạm Minh Thuấn

Hà Nội, 8-12-2023

**MỤC LỤC**

[CHƯƠNG 1. Chuẩn bị 2](#_Toc152945353)

[1.1 Mô hình 2](#_Toc152945354)

[2](#_Toc152945355)

[CHƯƠNG 2. Khai thác 3](#_Toc152945356)

[2.1 Phân tích Vuln 4](#_Toc152945357)

[2.2 Sử dụng robots.txt 4](#_Toc152945358)

[2.3 Tìm Flag 1 5](#_Toc152945359)

[2.4 Tải tệp fsocity.dic 5](#_Toc152945360)

[2.5 Bẻ khóa bằng Wpscan 5](#_Toc152945361)

[2.6 Đăng nhập vào WordPress 6](#_Toc152945362)

[2.7 Tạo PHP backdoor (Msfvenom) 6](#_Toc152945363)

[2.8 Tải lên và thực thi backdoor 7](#_Toc152945364)

[2.9 Kết nối ngược 7](#_Toc152945365)

[2.10 Nhận MD5 hash và giải mã tìm Flag2 8](#_Toc152945366)

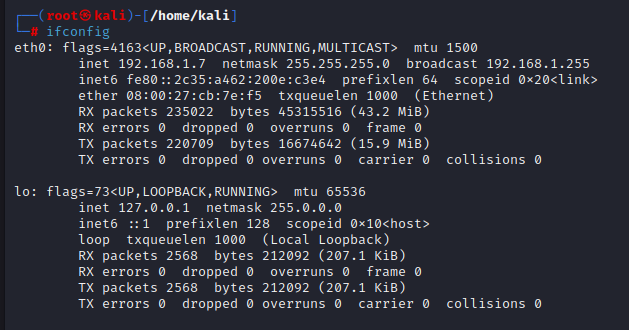
[2.11 Đăng nhập vào máy nạn nhân (Mr Robot) và tìm Flag3 8](#_Toc152945367)

# Chuẩn bị

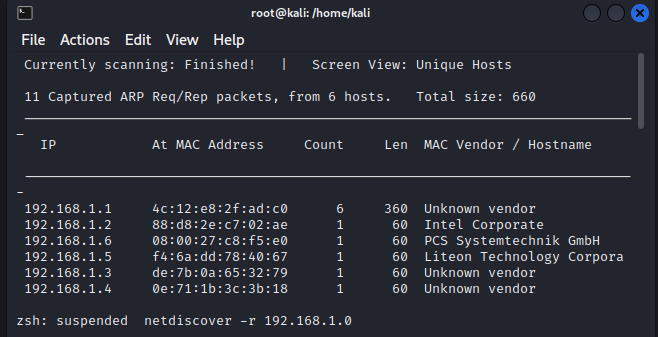
## Mô hình

## 

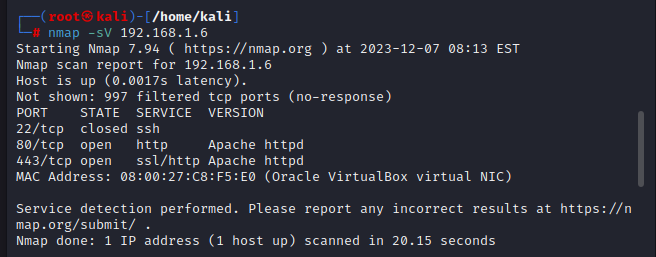
Địa chỉ ip của kali:



Quét các cổng để tìm máy nạn nhân (Mr Robot):

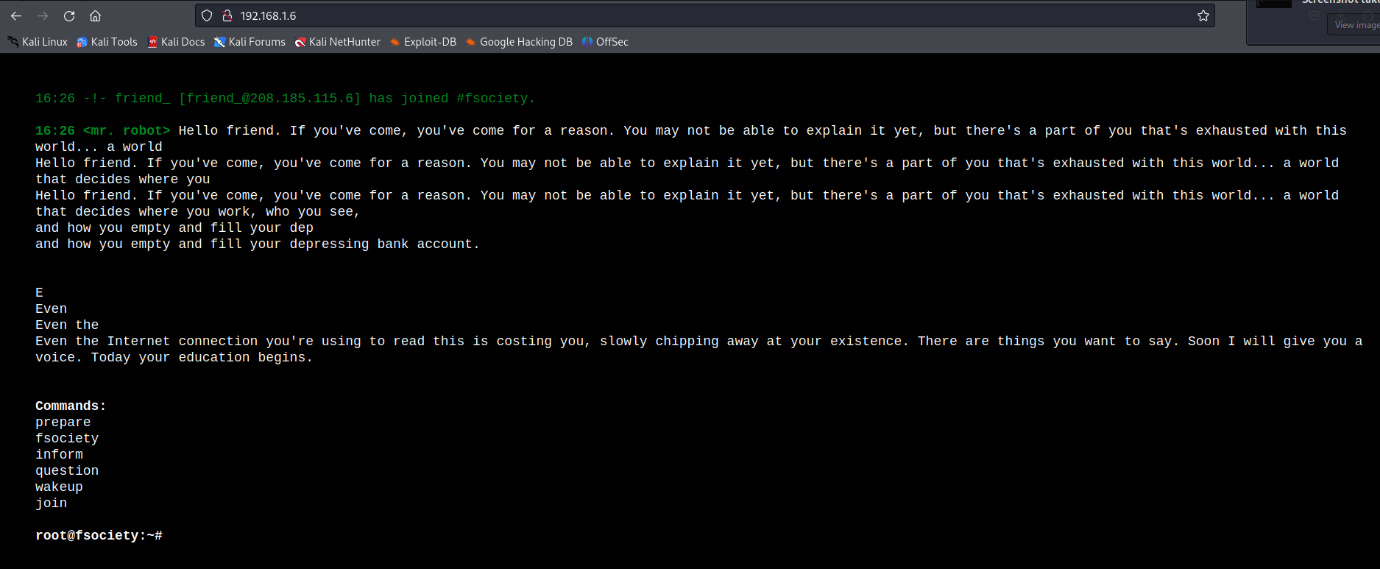


Nmap ip 192.168.1.6 để xem các dịch vụ , phiên bản, hệ điều hành:



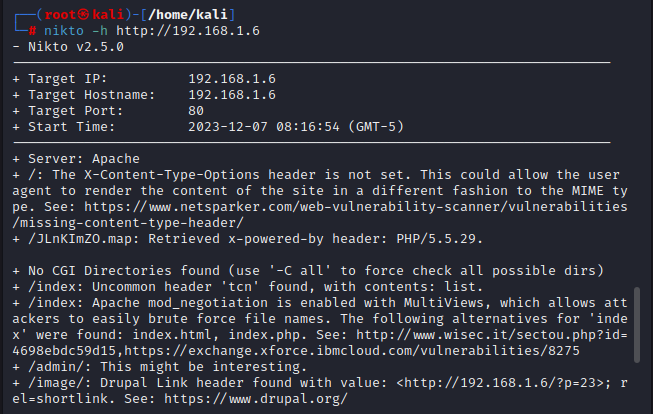
# Khai thác

Trang web của Mr Robot:



## Phân tích Vuln

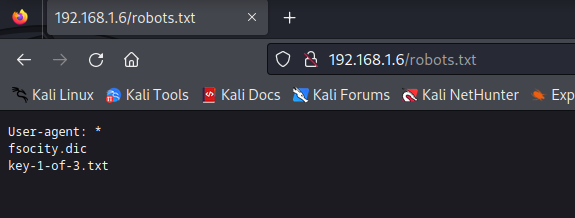
Nikto là một công cụ kiểm tra lỗ hổng bảo mật và quét web tự động. Nó được sử dụng để tìm kiếm các lỗ hổng phổ biến trong ứng dụng web và máy chủ web



=> Tìm file robots.txt

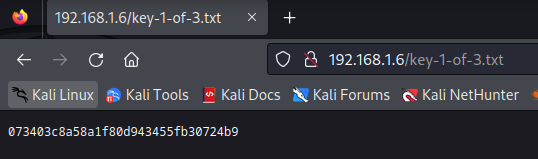
## Sử dụng robots.txt

Mở trình duyệt và nhập <http://192.168.1.6/robots.txt>



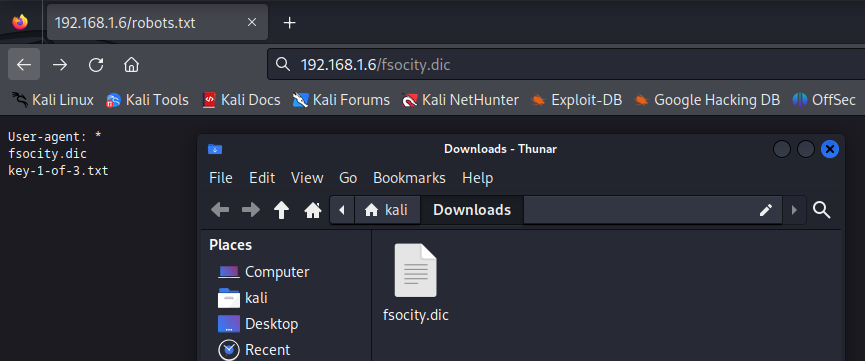
## Tìm Flag 1

Nhập <http://192.168.1.6/key-1-of-3.txt> để thấy Flag 1



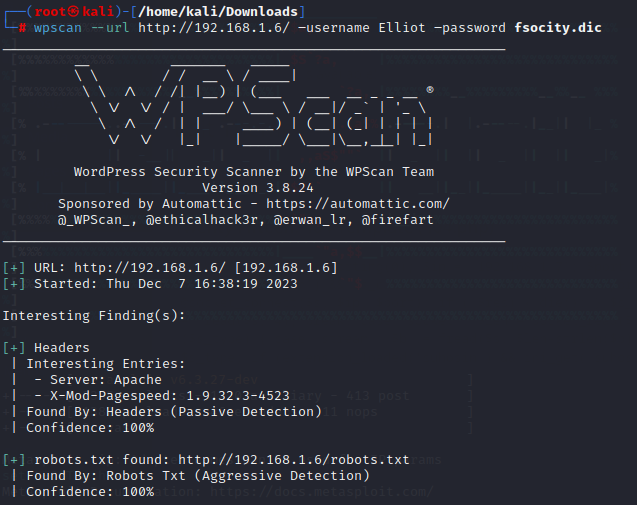
## Tải tệp fsocity.dic

Nhập <http://192.168.1.6/fsocity.dic> để tải tập tin



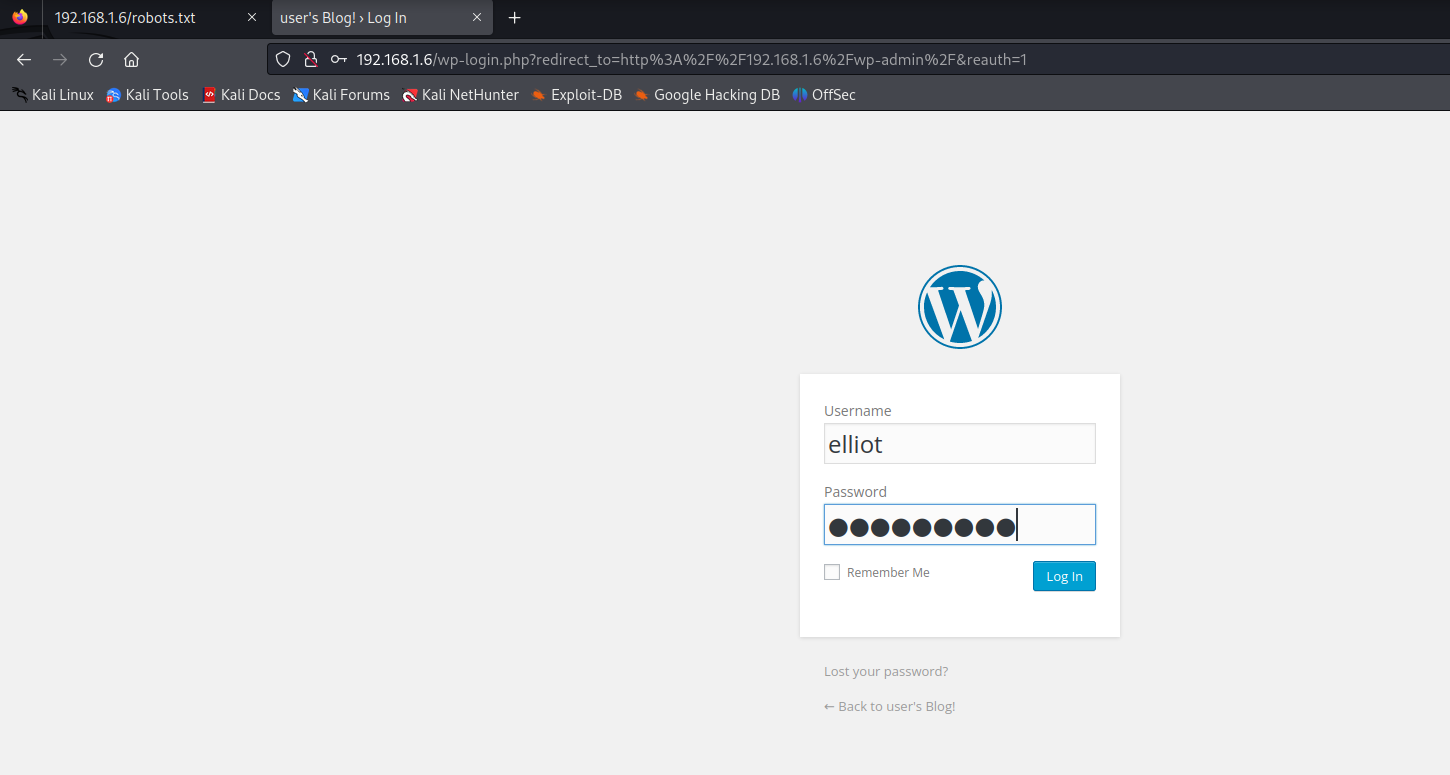
## Bẻ khóa bằng Wpscan

Sử dụng fsocity.dic để tấn công bruceforce tìm mật khẩu của WordPress

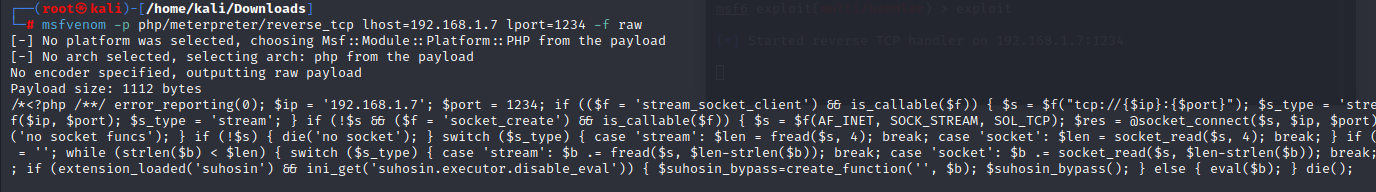


=> Pass: **ER28-0652**

## ****Đăng nhập vào WordPress****

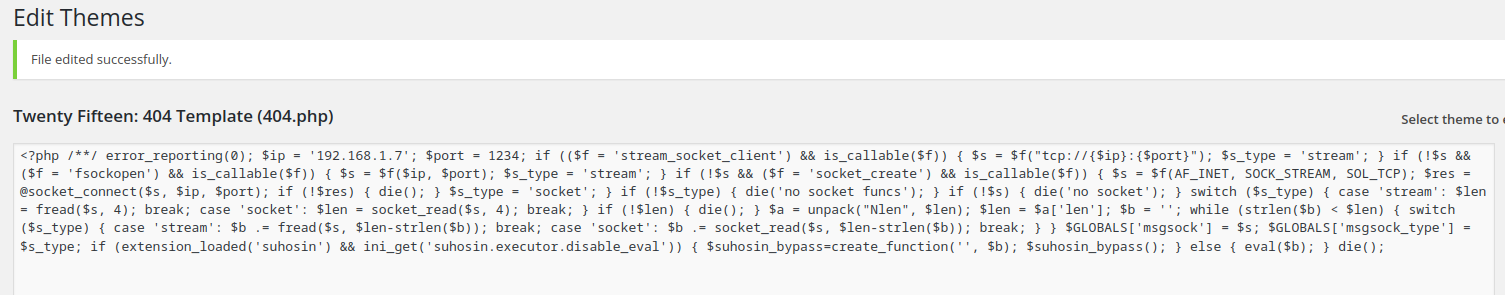


## Tạo PHP backdoor (Msfvenom)



## Tải lên và thực thi backdoor

Tải lên tại http://192.168.1.6/wp-admin/themeeditor.php?file=404.php&theme=twentyfifteen&scrollto=0



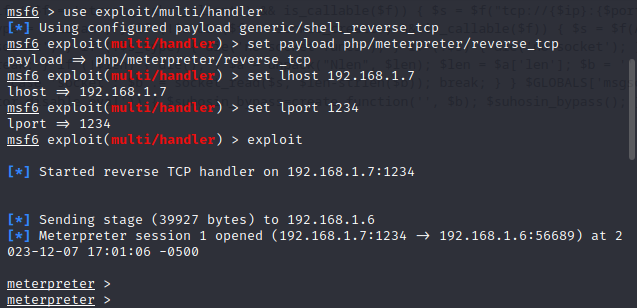
Rồi update file

## Kết nối ngược

Sử dụng exploit/multi/handler

Cài payload, đặt lhost là IP của kali, cổng tùy ý

Bắt đầu khai thác



Sau khi nhấp lại vào link <http://192.168.1.6/wp-admin/themeeditor.php?file=404.php&theme=twentyfifteen&scrollto=0>

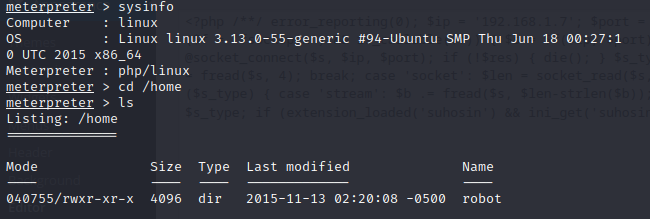
=> meterpreter shell mở

## Nhận MD5 hash và giải mã tìm Flag2

Sysinfo: xem thông tin

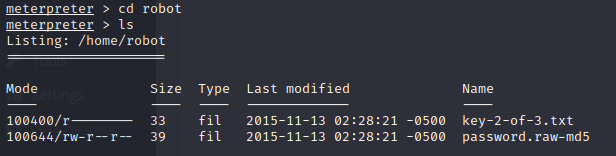
Chuyển hướng đến home

Xem danh sách=> có 1 file robot



Chuyển hướng đến robot

Xem danh sách có 1 khóa và 1 file mật khẩu chưa giải mã



Đọc file password.raw-md5



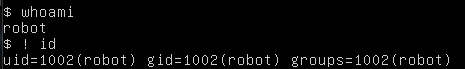
Mật khẩu md5 là **abcdefghijklmnopqrstuvwxyz (Flag 2)**

=> User, Password để vào máy:

User: robot

Password: **abcdefghijklmnopqrstuvwxyz**

## Đăng nhập vào máy nạn nhân (Mr Robot) và tìm Flag3



Nmap –interactive để chạy trong chế độ tương tác

Xem danh sách ở file root => file key-3-of-3.txt

Đọc file key tìm được Flag3

