

# 6iyp18php,2018-09-28-Vulnhub渗透测试实战writeup(4)

转载

有一失物 于 2021-03-20 00:26:07 发布 29 收藏

文章标签: [6iyp18php](#)

桥接到vmnet8网卡, 网段是10.10.10.1/24.

先主机存活探测, nmap -sn 10.10.10.1/24



图一

可以看到靶机ip地址为10.10.10.143

然后老规矩nmap和dirbuster扫描一波, 先nmap

```
sudo nmap -sV -A -p- -Pn 10.10.10.143
```

结果如下:

```
PORT STATE SERVICE VERSION
```

```
80/tcp open  http Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
```

```
|_ http-methods:
```

```
|_ Potentially risky methods: TRACE
```

```
|_ http-robots.txt: 3 disallowed entries
```

```
|_ /cola /sisi /beer
```

```
|_ http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
```

```
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

```
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: general purpose
```

```
Running: Linux 2.6.X|3.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
```

```
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13
```

```
Network Distance: 1 hop
```

可以看到只开放了80端口, apache版本2.2.15,php版本5.3.3,linux系统

接下来日常dirbuster扫描



图二

只能打开images以及icons目录，下面主要是一些图片文件，binwalk和gedit打开以后没发现有啥有价值的信息。

来到这一步就没辙了，只能看看有没有其他的入口点，仔细点看这幅图：



图三

他说：Keep caml and drink fristi.....

所以根据后面的提示，这个fristi可能是一个目录来着。。。好吧，ctf套路我也没啥办法。。

直接进入该目录看下。



图四

发现是一个管理界面来着。

想在这个目录下再扫描一波目录，结果发现全是403...

于是一波操作先下载图片,binwalk+gedit没发现啥

F12看看网页源码，发现一些注释



图五

这告诉我们里面有内联的base64编码的图片，以及作者的姓名，可能可以作为用户名登录。

然后编码如下所示：



图六

写了个简单的py脚本处理：

```
import os
import base64
s=""iVBORw0KGgoAAAANSUUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwlscAeBFjgDwlkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPI+zJO53b9+1gd/0TL2Wull5+RMpjQ5tMTkE1paHIVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORI72DbdWKqZS0tMPqGI8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
DpYzOMN1WqpILS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjILNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
```

```
12qmC/1/Zz2ZWXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFel5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqdg6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkq1
04VajmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUqOhEkso2k5pGy00aLq
i1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
tOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9IWvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4INOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++FI
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJI6o6+ech8dv0Uu4PnkqDI2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn/4+zfhV6aiilsczlGrGvGTllsLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYIm+hDLkclAtuHEUzu/I9I867X34
rPtA6lmLi0ZrqX6gu37alukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRlwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwlscAeBFjgDwlkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==""
```

```
imagedata=base64.b64decode(s)
```

```
file=open("1.png","wb")
```

```
file.write(imagedata)
```

```
file.close()
```

解码之后生成的图片如下所示：



图七

猜测一波，这可能就是密码了，还有上面的用户名。

试一下居然成功了。。。



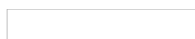
图八

看到这个就直接想到那啥了吧，上传漏洞，要么shell，要么菜刀一波。



图九

发现一波文件名上传限制，根据测试他只是检测了后缀名而已，因此没啥限制，直接把php的一句话木马文件改为jpg文件，然后直接上传后菜刀连接就可以了，如下：



图十



图十一

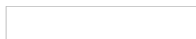
进去以后发现权限不是root，无法执行sudo,那就直接上python了,但是显示无法执行python???[黑人问号??]



图十二

然后尝试直接执行python -c看看，发现直接执行命令就可以生成伪终端了。

于是直接看看主目录下面有啥文件吧。



图十三

看到有一个关键用户eezeepz。

进去ls一下。



图十四

看到有一个note.txt,可能是作者的备注，暗中观察一波



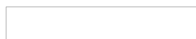
图十五

看看写了啥



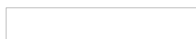
图十六

作者说了，可以在/tmp/目录下面创建一个文件runthis，然后把homedir里面的命令导进去，这里再次感叹一波真的需要学一学shell脚本，搞安全的真的啥都要会啊啊啊啊啊!!!



图十七

接下来看一下/home/下面的admin目录



图十八

除了几条命令以外，查看了cronjob.py明显是加载命令的py文件，另外一个cryptpass.py，看名字就知道是加密代码，cat一波：

```
import base64,codecs,sys
```

```
def encodeString(str):
```

```
... base64string= base64.b64encode(str)
```

```
... return codecs.encode(base64string[::-1], 'rot13')
```

这里是做了base64编码之后, 然后来个倒序, 接着用了rot13编码(其实就是13的凯撒加密), 然后我看了下两个txt文件, 都是加密后的编码, 那就直接上解码代码, 如下:

```
def decodestring(str):
```

```
... tmp=codecs.decode(str[::-1],'rot13')
```

```
... return base64.b64decode(tmp)
```

把whoisyourgodnow.txt解密, 如下:



图十九

解密出来为LetThereBeFristi!

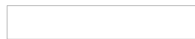
同样的cryptedpass.txt解密出来为:



图二十

解密出来为thisisalsopw123

这样的话可以猜猜是什么的密码了, 直接/etc/passwd一波



图二十一

可以看到介个用户名, fristigod等等, 几个用户名都试试一波, 发现fristigod是可以直接登录上去的。



图二十二

进去以后直接使用一波ls,发现啥都没有, 不合常理, 于是ls -la,解释一下,a是显示隐藏文件的选项。



图二十四

再探索一波



图二十五

发现了啥有一个叫doCom的文件是归属于root的

没啥线索, 再回前面history cat一波



图二十六

可以看到fristigod用户一直在尝试用sudo执行各种命令，我们看看他能执行啥命令，sudo -l是看当前用户能执行啥命令



图二十七

这里的密码仍然是LetThereBeFristi!，然后尝试生成shell

```
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom/bin/bash
```

这一步是模仿前面bash命令执行历史里面的命令来执行的。



图二十九



图三十

**Flag Get!**

总结：

- 1.主要根据线索来进入登录目录下
- 2.根据网页注释以及前端base64图片解码来登录
- 3.文件上传漏洞利用生成shell
- 4.利用python先生成伪终端
- 5.利用目录下的假面文件解密获取密码，然后再查看相应的可能用户尝试能不能su登录
- 6.登录以后尝试用ls -la查看隐藏文件，根据隐藏文件提示完成最终提权操作，获取flag