SWRhapsody

Buffer Overflow概念练习总结

于3月 3, 2018由**SWRhapsody**发布

因为是PWK课程提供的练习所以只进行简单记录

练习的是简单的32位程序的栈溢出，有关栈溢出的基本原理及部分进阶参考[1],练习的靶机是windows7，存在漏洞的程序是SLmail，这个程序负责提供对pop3支持，当登陆时密码位数过大时存在栈溢出漏洞。

这里主要记录总体思路，首先是确认漏洞的存在，用脚本与服务器交互找到发送多长的密码会使服务器不返回数据，再靶机上调试可以看见EIP、ESP都背覆盖了，再发送用kali中的pattern_create工具生成字符串找出可覆盖EIP的具体长度。

这个时候可以考虑利用漏洞，具体为利用漏洞来制造一个reverse shell。为了达成这个目的，我们需要将shell code上传到靶机，这个练习中shell code 会放在这超长的密码中比较好，因为测试中会发现这个漏洞一旦触发服务器中负责与你会话的进程会崩溃（这里有个奇怪的地方，每次在调试时崩掉发现slmail的那个控制器会告诉你slmail已经不存在了，但用netcat还是可以与110端口会话，完整exp会不起作用），shell code的存放位置有两种一种是shell code+NOP+EIP+负责跳转的code，另一种是NOP+EIP+shell code。

第一种的思路是复写EIP使他指向一段程序中已经存在的跳转到ESP的代码，再让负责跳转的code跳转到shell code，适用于覆盖太多会使程序崩溃的情况。

第二种的思路是复写EIP使他指向一段程序中已经存在的跳转到ESP的代码，让后就直接执行shell code。

在制作shell code之前要先测试是否存在bad character，如 `\r` 的 `\x0d` 会意外终止pop3的通信，这里教的测试方法是把 `\x00` – `\xff` 的字符都试一遍 `:(` ，有空看看有没有什么高效的方法。

这个练习是用第二种，用msfvenom生成shell的code，这里要注意使用压缩，一个是减少shell code的体积，第二个是为了绕过杀毒[2]。

SWRhapsody

参考及其他:

[1] CTF Wiki
[2] Rapid7 Blog

分类: EXPLOIT

0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

SWRhapsody

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

近期评论

文章归档

2020年8月

2020年6月

2020年5月

2020年3月

2020年1月

2019年12月

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

分类目录

相关文章

EXPLOIT

SWRhapsody

EXPLOIT

CVE-2020-5410

Introduction 补天挖的 spring-cloud-conf 阅读更多…

EXPLOIT

CVE-2020-1957

Introduction 这个漏洞需要1.5.2 版本以下的 shir 阅读更多…