小白言承之PWN学习路线（持续更新）

原创

书文winter 于 2020-01-29 16:39:28 发布 2562 收藏 101
分类专栏： CTF 文章标签： CTF 学习路线

本文链接：https://blog.csdn.net/qq_43935969/article/details/104107872

PWN（溢出）：PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。在CTF比赛中，线上比赛会有，但是比例不会太重，进入线下比赛，逆向和溢出则是战队实力的关键。主要考察参数选手漏洞挖掘和利用能力。

CTF PWN特点:入门难、进阶难、精通难

pwn学习内容：
（1）了解Linux ELF文件
（2）分析掌握栈溢出原理理解函数参数的传递过程栈空间变化
（3）掌握查找ROPgadget、32位和64位的exp构造
（4）掌握返回导向编程ROP，ret2libc、ret2_dl_resolve
（5）掌握linux系统延迟绑定机制：GOT、PLT查看libc库函数地址
（6）掌握堆溢出原理掌握动态内存管理malloc、free实现方法掌握堆溢出利用方法
　　（a）二次释放
　　（b）unlink技术利用
　　（c）释放后重引用漏洞
　　（d）fast binattack利用
　　（e）house of 系列利用
　　（f）unsorted bin attack利用
　　（g）函数hook地址覆盖
（7）理解格式化字符串原理
（8）理解竞争条件漏洞
（9）理解整数溢出原理
（10）了解常用系统保护措施：checksec（-NX-canary-RELRO–PIE）
（11）了解保护措施相关绕过方法
（12）SSP 泄露利用泄露
（13）canary利用

【参考铁人三项考纲】

之前学习东西比较杂，经过一段时间的学习，有点feeling了。这里主要记录下自己的学习历程，仅供大家参考。

（1）首先是汇编基础：王爽的《汇编语言》

（2）滴水公开课：https://www.bilibili.com/video/av20193835?from=search&seid=5407506588268642108（主要是为了了解函数调用过程）

（3）攻防世界刷题：https://adworld.xctf.org.cn/personal

（4）君莫笑视频：https://space.bilibili.com/14500640/

（5）《0day安全：软件漏洞分析技术》

（6）CTF-Writeup Github刷题:http://github.com/ctfs

（7）CTF - Wiki：https://ctf-wiki.github.io/ctf-wiki/

（8）Linux内核：https://www.bilibili.com/video/av47154483?p=1

（9）堆：https://ctf-wiki.github.io/ctf-wiki/pwn/linux/glibc-heap/heap_structure-zh/（ctf-wiki基础概括的比较全了）

（10）这篇博客各种利用技巧讲的比较好：https://www.lhyerror404.cn/2019/01/22/heap-exploitation%e7%ae%80%e4%bd%93%e4%b8%ad%e6%96%87/

（11）《glibc内存管理ptmalloc源代码分析》

（12）大杂烩：https://github.com/CHYbeta/Software-Security-Learning

（13）glibc里的one-gadget：https://xz.aliyun.com/t/2720

【`one_gadget /lib/x86_64-linux-gnu/libc.so.6`】libc_base_address—>one_gadget_address

【查看程序中的函数：readelf -r easyR0p】

【**ldd命令**用于打印程序或者库文件所依赖的共享库列表。】

HOF:https://bbs.pediy.com/thread-222924.htm

（14）堆的简单利用：https://www.freebuf.com/articles/system/151372.html（这个一系列写的真心好，强推！）

（2020.1.29）言承将栈溢出这块差不多比较清楚了，接下来往堆溢出方向学习。

（15）学习内核

操作系统知识：https://next.xuetangx.com/learn/THU08091000267/THU08091000267/4215533/video/6084206

并完成相应的练习。