CTF逆向选手的自我修养

r3kapig – 申奥成

自我介绍

- 常用ID Pizza
- 深圳大学本科在读
- 18年开始接触CTF, 在此之前有多年逆向实战经验
- r3kapig主力逆向选手, 参加过多次CTF大赛并取得优异成绩

逆向工程

软件逆向工程是一种探究应用程序内部组成结构及工作原理的技术. 运用逆向分析技术, 窥探程序内部结构, 掌握其工作原理. --《逆向工程核心原理》

在CTF中, 逆向题目除了需要分析程序工作原理, 还要根据分析结果进一步求出FLAG.
逆向在解题赛制中单独占一类题型, 同时也是PWN题的前置技能.
在攻防赛制中常与PWN题结合.

基本能力

掌握汇编语言(x86, arm, mips, ...)与一定的软件开发经验

代码内的: 算法, 数据结构, 设计模式...
代码外的: 可执行文件格式, 编译原理, 操作系统...

逆向开发套件: capstone, keystone, unicorn, pefile, LIEF...

工具使用

逆向分析必然要和各种专业工具打交道, 对工具的使用熟练程度, 也是逆向能力的一部分.

- 专业逆向工具往往集成了多项功能, 除了最主要的功能外, 还应了解工具内其他辅助分析的功能, 以及熟记各种快捷键.
- 大概了解工具原理, 了解工具中各种设置选项的影响, 调整工具满足使用需求.

工具使用

- 除了工具本身, 其所支持的插件也值得关注. 插件是对工具自身功能的补充与扩展, 也可以修补工具的一些缺陷.
- 善用脚本开发接口, 通过脚本能够十分方便地利用工具中的一些高级功能与分析结果进行自动化的逆向工作.

题型考点

CTF中的逆向题目有一下几个常见考点

- 常见算法与数据结构
  - 各种排序算法, 树, 图等数据结构
  - 识别加密算法与哈希算法代码特征,识别算法中魔改的部分
- 软件保护技术
  - 代码混淆, 代码虚拟化, 自修改代码, 反调试等
  - 软件加密壳是软件保护技术的集中应用
  - 大部分技术都有开源的实现, 通过学习实现, 掌握对抗技巧

题型考点

- 游戏博弈, 接口协议
  - 将游戏或玩具的逻辑用代码实现, 逆向首先要找到程序的原型, 将程序数据转换为游戏信息, 再依照规则解决游戏.
  - 以正常调用程序, 达到某种状态或调用部分功能为目标
  - 迷宫, 魔方, 扫雷, 井字棋, 传奇霸业. FTP下载文件, 用户登录, GDB调试协议.

解题技巧

- 逆向与猜测结合，通过逆向缩小猜测范围，猜测为逆向指出方向，逆向再验证猜测的思路.
- 结合代码上下文与整体程序功能，关注程序中给出的文字提示信息.
- 实际比赛中逆向题目多数是为出题而出题，有目的性强，功能结构单一，无关代码少等特点.
- 遇到程序代码量极大时，可以先判断是否引用了较多的开源代码，而主逻辑相对简单.

保持耐心

- 逆向本身就是体力活, 需要长时间的努力.
- 及时总结当前已分析的结果, 指出目前遇到的困难, 寻找下一步的努力方向, 形成循环.
  - 找不到数据流与控制流或跟丢, 分析线索中断
  - 遇到软件保护技术, 代码量工作量大
  - 未知的算法, 数据结构
  - 未知的文件格式, 指令集, 无从下手

比赛心得

参加比赛, 最直观的肯定是参赛成绩.

- 0CTF/TCTF 2019 决赛第一名
- WCTF 2019 第三名
- *CTF 2019 第一名
- RCTF 2019 第一名
- 第三届强网杯全国网络安全挑战赛 第四名
- 第十二届全国大学生信息安全竞赛 初赛第五名

比赛心得

以赛代练

- 通过做题锻炼解题能力
- 在解题过程中暴露知识盲区，查漏补缺
- 提供动力促使选手学习
- 从题目中了解新兴的技术

比赛心得

选择比赛

- 根据比赛背景, 主办方与出题团队, 以及ctftime或ctfrank上的评分判断比赛质量
- 依照个人能力, 比赛难度循序渐进
- 出题人与参赛选手之间的技术交流, 不仅是考验选手对现有知识的掌握

谢谢观看

THANKS