非典型安全研究人员的自我培养

李冠成 Atum

About Me

- Atum, Guancheng Li
  - http://atum.li
- CTF Player:
  - Captain of Eur3kA, r3kapig
  - Previous member of blue-lotus, Tea Deliverers
  - DEFCON 25/26/27 CTF
- Experience
  - Master @ICST SECLAB, Peking University
  - Researcher @ XuanWu Lab, Tencent Security
- Keyworks
  - RE/PWN/Hacking/R&D

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

初始状态

- 大四
- 有一定的编程基础
  - NOIP 一等奖, ACM/ICPC 银牌
- 有一定的科研经历
  - ACM CCS 论文一篇
- 软件/系统安全初学者
  - 只调过0day安全书里的栈溢出。不太会用IDA

中间状态1

- 研一
- 二进制安全入门
  - 可以解决大多数国内比赛的libc PWN题，能够看懂大多数漏洞分析
  - 非libc的PWN一脸懵逼，逆向题不会做。挖不到漏洞
- 知识面扩宽
  - 了解了一些有趣的东西，如coverage guided fuzz, CFI, Adversarial Deep Learning
- 瓶颈
  - 逆向能力不足

中间状态2

- 研二
- 二进制安全进阶
  - CTF转逆向，因而逆向基本功得到迅速提高，轻松挖非主流目标的漏洞
  - 对PWN有了系统观和大局观
  - 不知道怎么挖主流目标的漏洞
- 继续扩宽知识面
  - 参加了一年的清华组会，了解到了很多state of the art的研究成果，感谢张超老师提供的平台
- 瓶颈
  - 开发能力不足，长期研究能力不足，非熟悉的事物学习较慢

中间状态3

- 研三
- 二进制安全进阶
  - CTF转MISC，一定程度上锻炼了非熟悉事物的学习能力
  - 对主流目标的漏洞挖掘方法有了一定的认知，但未实践
- 专注课题研究
  - 开发能力有了一定的提升，长期研究能力提升
- 瓶颈
  - 计算机基础知识有待恶补（编译、操作系统等）
  - 开发和架构能力仍有待提高（编写高质量项目代码）

进步是怎么来的？

- 根源
  - 扎实基本功，不断学习和了解新事物
- 过程
  - 科研(20%)
  - 瞎研究一些没用的(20%)
  - 打CTF(20%)
  - 因为CTF打的太累而划水(10%)
  - 娱乐(15%)
  - 上课(15%)

扎实基本功

- 搜索能力
- 代码/文档等的快速阅读
- 逆向工程
- 脆弱点/问题的挖掘和利用
  - 对漏洞的感觉和挖掘思路
  - 漏洞利用的思路
- 正向开发能力
- 沟通和社交

为什么是基本功?

- 搞研究是做什么呢?
- 发现问题
  - 寻找可以做的点?
- 解决问题
  - 搜索/学习 不熟悉的知识
  - 逻辑思考

发现问题 vs 解决问题

- 发现问题
  - 微观：找软件脆弱点 等
  - 宏观：找未被解决的问题/找现有方法的不足 等
- 解决问题
  - 漏洞这么多，怎么办？
    - 统一开发SDK，规范开发流程
  - 研究解决方案/改进方法

真实的情况是...

- 发现不了问题
  - 挖不到漏洞
  - 找不到可做的点
- 发现了问题，但不知如何下手解决
  - afl-fuzz 搞自定义协议效果不好，咋改进
- 知道该做什么但是效率太慢
  - 研究一个防护机制，写llvm parser 写一个月
  - 写一个内核上的解决方案写了好久。。

问题出在...

- 基本功不好！
- 假设你是这样的...
  - 读代码读的贼快
  - 人肉逆向机
  - 搞过很多东西，随意魔改过操作系统
  - 代码能力很强，想写啥写啥
  - 平时的工作就是不断之前解决不熟悉的问题，学习新知识，知识面丰富

进步是怎么来的？

- 根源
  - 扎实基本功，不断学习和了解新事物
- 过程
  - 科研(20%)
  - 瞎研究一些没用的(20%)
  - 打CTF(20%)
  - 因为CTF打的太累而划水(10%)
  - 娱乐(15%)
  - 上课(15%)

What do you think of CTF

- 都是套路，没啥意思
  - 菜单题，add, delete, edit 一番操作拿shell
- 跟真实攻防差距很大
  - CTF玩的6，搞真实软件一脸懵逼
- 搞时间长了没意义
  - 初学时搞搞玩，入门了就做科研

- Fake CTF!

打真正的CTF!

- 大佬们都在打CTF
  - Niklasb, Lokihardt, riatre, yan, sealo etc..
- 图啥？
- CTF促进研究能力！

Real Capture The Flag!

- Reverse/Pwnable/Web/Crypto/MISC
- 高质量的CTF比赛：
  - DEFCON CTF/C3CTF/HITCON CTF/0CTF/Plaid CTF/WCTF
  - 由国际顶尖安全团队设计 (腾讯科恩、360Vulcan、LegitBS、PPP等)
  - 赛题质量高
- 解题
  - 知识盲区 70%-100% 快速学习能力
  - 知识盲区 0-30% 其他能力训练

什么是高质量的CTF题目

- https://zhuanlan.zhihu.com/p/67785521

1. 智障赛题：考察点为无意义的脑洞，或考察点太过于简单。
2. 辣鸡赛题：考察点有难度却较为无聊。
3. 初级赛题：主要考察对主流技术的掌握和灵活应用。
4. 中级赛题：满足初级赛题的条件，但难度相对较高。
5. 高级赛题：赛题的考察点对于绝大多数选手来说都是陌生且足够有趣。出题人通过对赛题进行精巧的设计，从而使得做题过程中可以一步一步被引导学习到出题人想要分享的有趣的idea和知识。高级赛题一般来说都比较有难度（毕竟要学很多新东西），却难的合情合理。
6. 顶级赛题：满足高级赛题的条件，且赛题难度和步骤设置合理，能够及时的让做题人得到及时反馈和成就感。

高质量CTF赛题的外在特点

- 考点杂，覆盖面广、富有挑战性
- 从传统的二进制/WEB安全 到较新的物联网安全、区块链安全、AI安全等
- 最新防护机制的绕过、各种平台的漏洞利用、最新顶会顶刊论文的实现、自定义混淆算法的解混淆、密码算法安全性分析、各类很杂的知识点、黑盒分析

几个例子

- DEFCON 26 CTF: multi-arch shellcode
- DEFCON 27 Quals: hotel california, trace系列
- 0CTF 2019: vim/wasabi系列
- 34C3 CTF: LFA
- 做题过程
  - 找可能的脆弱点
  - 搜论文，搜文档，学之
  - 解题
  - 断网可就做不出来了

通过打高质量CTF接触到的点

- 区块链/机器学习等跨领域热门技术
- 各种fancy的硬件特性 Intel SGX, Intel PT/BTS/LBR
- 信号分析/各种各样数学知识
- 各种奇怪的语言的逆向和代码阅读
- 各式各样平台的漏洞挖掘和利用
- 快速阅读代码和项目
- 不断的学习新东西。。

打高质量CTF的其他好处

- 合法致富
  - 命题！培训！比赛奖金！
  - 对代打说no！
- 认识很多志同道合的大佬
- 绝对硬核，收益稳定，童叟无欺
  - 货真价实的基本功
  - 货真价实的知识面
  - 货真价实的学习能力
  - 货真价实的战友和技术大咖

可能会遇到的陷阱

- 大家都觉得我是大佬
  - 名不符实，未妥善平衡好名和实的关系
- 搞过很多东西
  - 大多数都蜻蜓点水，深度探索和广度探索很不一样
- 在高质量比赛(如DEFCON)拿了很好的名次
  - 全靠大佬队友带
- 拿了很多大奖和奖金
  - 某杯某杯，都是考察知识的熟练度。
  - 拿着现有的随便项目改改参赛

可能会遇到的陷阱

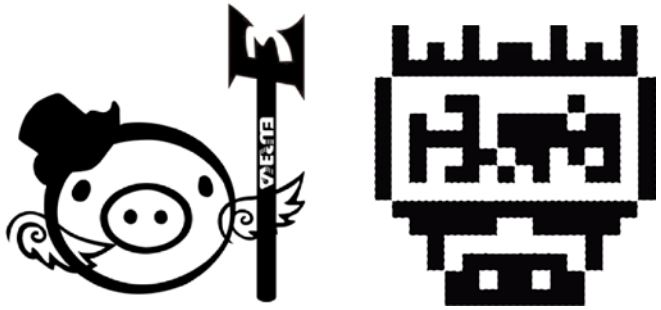
- 挖了很多漏洞
  - 找了个开源fuzzer 跑了一波
- 写了很多代码
  - 没啥难度的业务逻辑代码
- 认识了很多大佬
  - Twitter 社交达人
- 掌握了各种各样的技术
  - 只掌握了上层的技巧，实际基本功很差

总结

- 扎实基本功
- 持续学习新事物
- 在至少一个值得专注的课题深耕
- ~~适度包装和PR~~

额外的

- 欢迎加入r3kapig战队
- r3kapig.com



Selected Awards

Game Name	Time
DEFCON 26 CTF Final, 18th place	Las Vegas, USA, Aug. 2018
Nuit du Hack CTF Quals 2018, 5th place (JD-r3kapig)	Online, Oct. 2018
Real World CTF 2018 Quals, 3rd place	Online, July. 2018
XCTF 2018 Final -HITB BEIJING, 1st🏆place	Beijing, China, Nov. 2018
BCTF 2018, 1st🏆place	Online, Nov. 2018
Real World CTF 2018 Finals, 5th place	Zhengzhou, China Dec. 2018
Trend Micro CTF 2018 Finals, 4th place	Tokyo, Japan, Dec. 2018
0CTF/TCTF 2019 Quals, 5th place	Online, March. 2019
*CTF 2019, 1st🏆place	Online, April. 2019
RCTF 2019, 1st🏆place	Online, May. 2019
0CTF/TCTF 2019 Final, 1st🏆place	Shanghai, China, June. 2019
WCTF 2019 Onsite(Master), 3rd place	Beijing, China, July. 2019

Thank you

Questions are welcome