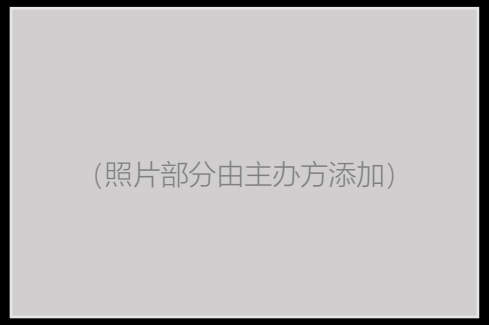


打造CTF+“肾”透测试攻城狮兴奋混合剂

孔韬循（K0r4dji）　赛宁网安攻防实验室总监

自我介绍

姓名：孔韬循

ＩＤ：K0r4dji

擅长：Web安全、渗透测试、团队管理、团队运营、安全产品原型设计等

成长：最早自学并接触安全在2008年-2009年期间至今。

年龄：90后

名言：没有高手和菜鸟，只有玩的多和少！

学历：本科（非统招），因高中中途辍学…走上信息安全”不归路”

其他：业余时间经常公益性质帮助非职业白帽、野路白帽转向正规军

外号：猥琐K、猎头K、启蒙K、逗比K、导师K…（此处省略网友送的N个外号）

- 国内白帽安全研究团队-破晓团队（Pox Team）创始人
- 中央企业-中国电子CEC-可信华泰教育事业部-技术专家顾问
- 中国工信出版集团-人民邮电出版社-IT领域图书资深专家顾问
- 中国工信出版集团-电子工业出版社-《Web安全深度剖析》书籍辅助修改者
- 中国工信出版集团-电子工业出版社-《Python带我起飞》专家书评撰写者
- 中国工信出版集团-人民邮电出版社-《Windows黑客编程技术详解》专家书评撰写者
- 中国工信出版集团-电子工业出版社-《内网安全攻防：渗透测试实战指南》专家书评撰写者
- 北京大学出版社-《SqlMap从入门到精通》专家书评撰写者
- Freebuf-2019-FIT-白帽LIVE论坛议题讲师、XCTF-Xman上海站高级讲师
- 第二届”强网”拟态防御全球国际精英挑战赛官方赛事解说员
- 第二届强网杯三等奖、第三界强网杯官方赛事嘉宾&解说员
- 2019网络安全“金帽子”奖年度盛典-专家评审团评委（嘶吼）
- 广州大学/北京邮电大学-方滨兴院士班-CTF+渗透测试实战夏令营/冬令营高级讲师
- 北京蓝森科技-15PB实地信息安全培训机构-特聘讲师

网络安全创新大会
Cyber Security Innovation Summit

目 录

CONTENTS

渗透测试发展历史-技术

2005年

05-10年会使用脚本的人非常多。

脚本小子时代

2010

高级脚本小子时代

10-15年，制作脚本的人越来越多

2015

2015-至今，人才复用+全栈

信息安全工程化

至今

白帽第三方平台：

乌云/漏洞盒子/补天等

SRC应急响应中心平台：

ASRC/BSRC/TSRC等

乙方各路公司：

天融信/绿盟/启明/360等

各路安全团队：

安卓/Web/IOT等

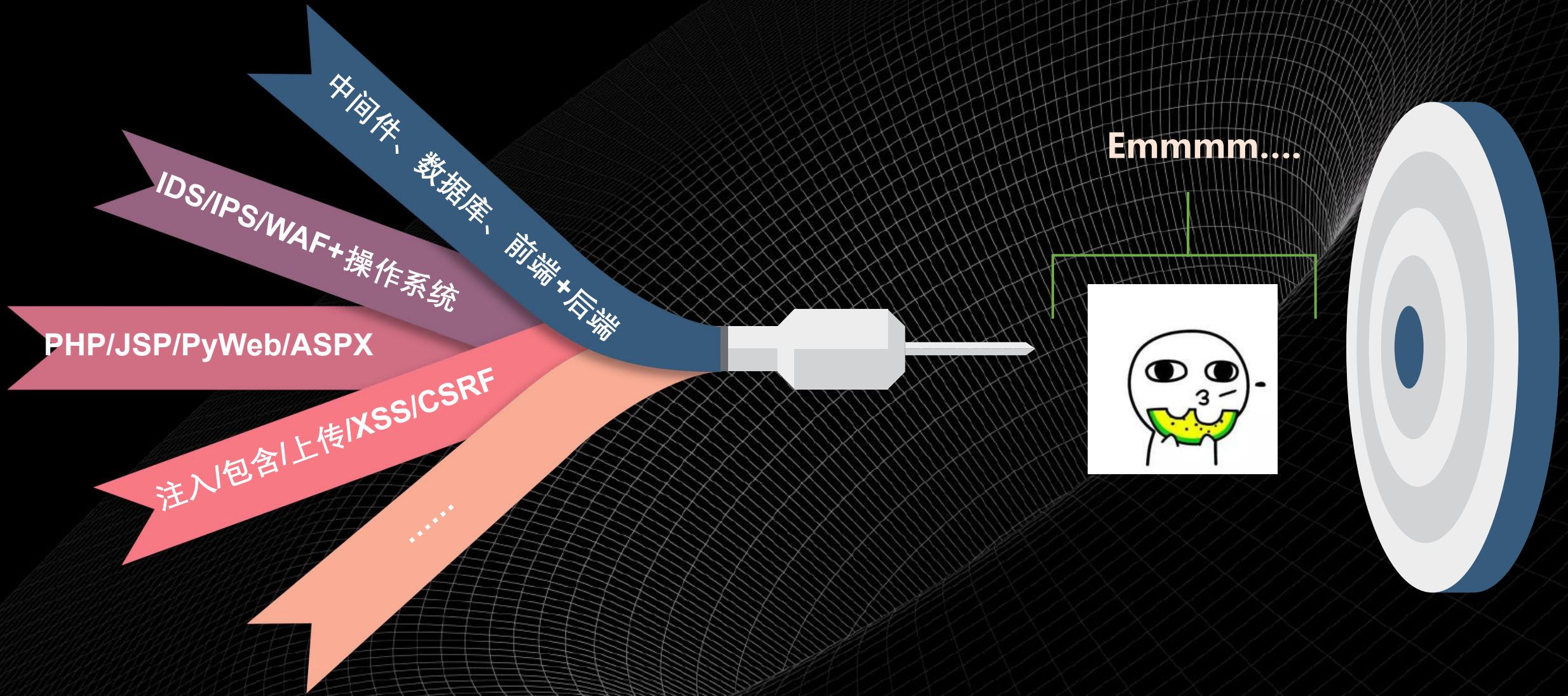
其中借助：文章、视频教程、社区论坛、社交软件QQ等方面收货了知识和队友。

安全技术相关论坛/社区/团队等（列部分）排名无先后

- 黑客风云
- 黑客动画吧
- 红黑联盟
- 黑客基地
- 饭客网络
- 华中帝国
- 小七论坛
- 新世纪网安
- 郁金香辅助
- 独立团辅助
- 外挂海论坛
- 360安全客
- Linux520
- 黑客反病毒
- 黯势黑客联盟
- 邪恶八进制
- 幻影旅团
- 绿色兵团
- 红客联盟
- 80sec Team
- 黑客武林
- 黑白网络
- 黑鹰基地
- 暗影安全
- 吾爱破解
- 看雪论坛
- T00ls论坛
- 冰客安全
- 小甲鱼安全
- 夜鹰安全
- 暗组安全
- YES黑客联盟
- 学生黑客联盟
- 黑客防线
- 黑客X档案
- 黑客手册
- 独特论坛
- 华夏黑客联盟
- 乌云网
- Freebuf/漏洞盒子
- 90Sec Team
- 滴水逆向
- Sh3llC0de安全
- Backtrack中文网
- 黑狐安全网
- 中华隐士
- 黑客联盟
- 资源共享吧
- 黑客共享吧
- 暗组安全
- 库带计划（补天）
- 看雪论坛
- 黑盾论坛
- 小甲鱼论坛
- 甲壳虫论坛
- 黑手安全网
- 华中红客
- HACK80论坛
- 南域剑盟
- 0x557安全团队

CIS 网络安全创新大会
Cyber Security Innovation Summit

求距离？求速度？求高度？求阻力？



渗透=肾透

JavaWeb开发工程师

安全运维工程师

Windows安全工程师

Web安全工程师

数据库工程师

PHP开发工程师

无线安全工程师

Linux安全工程师

移动安全工程师

协议分析工程师

二进制反病毒工程师

IOT安全工程师

代码审计工程师

Python开发工程师

求求你，别
让我学了，
我跑不动了！

上班一般都忙啥?

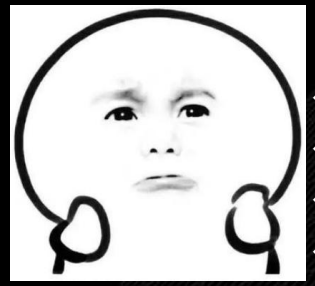
- 应急响应：系统访问不了啦，被黑客入侵了…
- 现场讲课：客户需要安全培训…
- 代码审计：需要对系统进行白盒代码审计…
- 安全研究：漏洞挖掘、各种研究…
- 工具编写：编写各种EXP/POC自动化Py代码…
- 报告撰写：应急报告、渗透报告、漏洞验证报告…
- 渗透测试：Web漏洞、内网渗透…
- 驻场服务：去客户那里上班….外派出去服务…如：护网行动！
- CTF比赛：强网杯、XCTF、网鼎杯、各种CTF…
- 新洞跟进：复现中间件漏洞、CMS漏洞、数据库漏洞、操作系统漏洞…
- ……（取决你的公司、你的部门、你的领导…）

技术成就感拉高与维持困难

找到突破口或迷失方向！

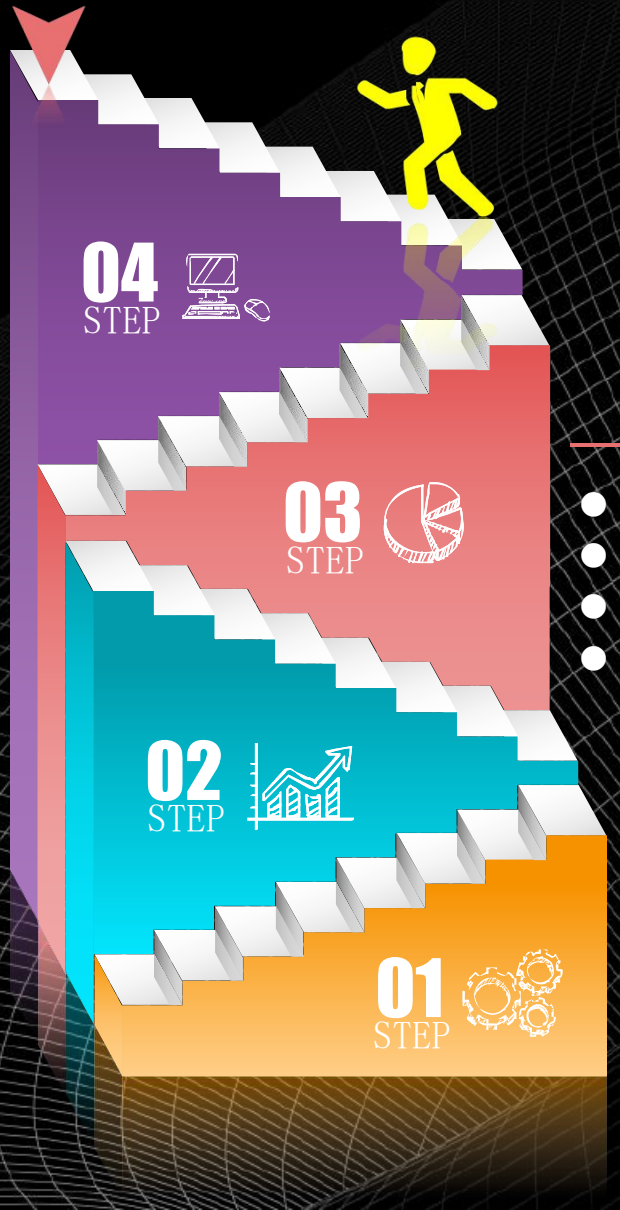
成就感不连续

- SqlMap的红色error
- 渗透中的“灵异”事件
- 系统没漏洞（硬找）
- ....



各种知识盲区

- 视频里的知识实战不好用
- 大佬给的思路我也看不懂
- CTF里的知识渗透用不了
- ...



五花八门的漏洞方向

- 数据库漏洞：提权、泄露...
- 安卓的漏洞：脱壳、逆向...
- 中间件漏洞：上传、溢出...
- ...

兴高采烈的学习信息安全

- 总觉得安全非常炫酷，B格高
- 能玩的知识领域很多，很开心
- 漏洞复现成功率真高，超开心
- ....

零散知识建立体系无从下手（乱的跟坦克大战一样！！）

CIS 网络安全创新大会 Cyber Security Innovation Summit

SQL注入

Kali Linux

SqlMap

SSRF

AWVS

AppScan

Metasploit

端口服务

Nmap

Whois

CSRF

脱壳

文件上传

命令执行

暴力破解

FTP提权

目录探测

未授权访问

银票据

免杀处理

子域名

金票据

目录遍历

端口复用

端口转发

GetShell

数据库提权

逻辑漏洞

任务攻坚较为困难-人才断层（两极分化）

渗透？扫描器扫一下导出个报告，下班了？

01

有一些经验可以挖出部分漏洞与安全隐患。

02

人呢？

04

各种大佬在研究…

05

巨牛逼，不知道牛在哪

公司培养好了，辞职了！ 中间环节缺乏沟通的桥梁与粘合剂！ …

任务攻坚较为困难-领导管理出问题

- 领导不懂技术，指挥容易自嗨。如：明天给我来个Windows 10远程溢出,挖个虚拟机逃逸不就OK了！
- 领导没有责任，不会安抚手下。如：能者多劳嘛。（完了？后面呢？就甩我一句话啊？）
- 领导不会谈心，技术性格内向。如：别走啊，一起玩啊（手下不会跟你说实话，害怕你！也很内向）
- 领导不知担当，任务胡乱派发。如：那个谁，你把XX任务做下（哇靠，怎么老是做别人部门 的任务）
- 领导不懂分享，较喜欢吃独食。如：今天我完成了XX业绩（我？我们？好像不在一个次元！）
- 领导不懂保护，任意其它甩锅。如：经常替别的部门背锅（莫名其妙的无数个锅就漫天而飞！）
- 领导不懂挽留，画饼过于严重。如：哎呀，明年上市了就（画饼太多，容易吃吐手下！）
- 领导没有优势，手下易不信任。如：我们领导啥都不懂（缺乏沟通和感情培养与成就感！）

感觉环境多样化-易迷路（渗透群体经常聊的那些事儿）

对话一：别学C，学Java，学PHP，学Python

对话二：你看某大忽悠技术啥都不会，都年薪百万了

对话三：学网络安全吧，挣钱多

对话四：别学网络安全，工资还没美工UI、开发高

对话五：学写PPT吧，比搞技术地位高，还易当管理

对话六：你看某家公司的渗透都40K的薪资了

对话七：刚毕业找网安就得不能低于10K，要不然活不下去

对话八：学渗透吧，比二进制安全有前(钱)途

对话九：还是自学好，别报培训班了，浪费钱

对话十：网络安全不看学历，没事，我们一起辍学

……

网络安全创新大会
Cyber Security Innovation Summit

目 录

CONTENTS


网络安全巡回赛 新加坡站


MOBILE
K 神

01 CTF预置了已知漏洞

02 渗透测试挖掘未知漏洞

03 CTF模拟了大部分攻防手法

04 实战渗透学习被大量限制

- AWD攻防模式简介AWD：Attack With Defence，你还得会修防，还得会攻。
- CTF传统解题：题目一个个的破解即可。
- CTF运维赛：以运维工程角度PK安全技能为主。
- CTF个人赛：以个人为单位，进行相关模式的PK。
- CTF团体赛：以多人为单位，进行相关模式的PK。
- …

多元化CTF-WEB

CTF-WEB能拿Flag的点有很多，分别从低中高三个档次不等

- 前端HTML查看源代码
- 多次编码解密
- HTTP协议头修改
- 用Python比速度
- 绕过安全保护机制
- …

WEB安全测试能找到的漏洞难度也不一样，如：

- 银行系统
- 商城系统
- OA办公系统
- 人力资源系统
- 邮件系统
- …

中间件的基础：Apache、IIS、Nginx、WebLogic、Tomcat等

数据库的基础：Oracle、MySql、SqlServer等

编程语言基础：PHP、Python、PythonWeb、Java、JavaWeb等

安全漏洞基础：XSS、CSRF、SSRF、SQL注入、文件包含、URL跳转等

安全手段基础：信息收集、暴力破解、端口转发等

WAF绕过基础：安全狗、护卫神、360、D盾等

漏洞工具基础：Nmap、SqlMap、BurpSuite、Metasploit等

题目脑洞基础：（无法用语言形容，看汗水和智商！）

代码审计基础：PHP代码审计、PythonWeb代码审计、JavaWeb代码审计等

权限提升基础：第三方组件提权、FTP提权、数据库提权、Shell提权等

CTF-RE

- 可逆向，代码量大部分不是很大。
- 大部分是已知的算法和世面上已知的壳

表示学校里从来不教这个

工作中的RE

- 逆向代码量大的吓人
- 未知的壳、未知的算法

编程语言基础：C/C++、 x86汇编、x64汇编等

分析工具基础：OD、IDA、Windbg、gdb等

操作系统基础：Windows API、Windows内核、Linux内核等

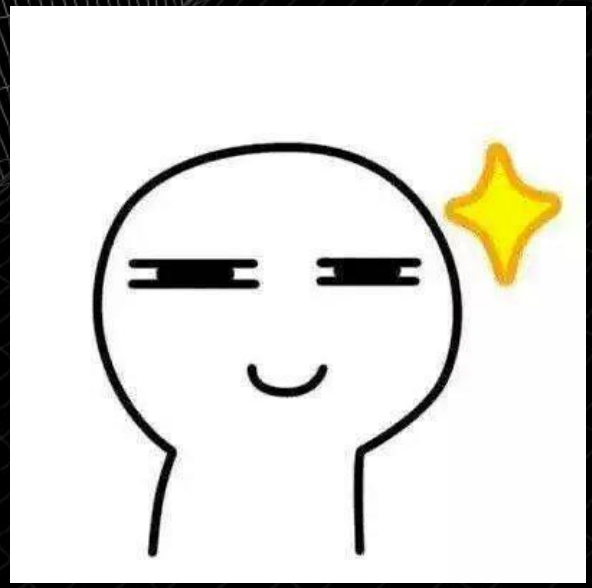
文件结构基础：PE文件结构、ELF文件结构等

文件脱壳基础：压缩壳、混淆壳、加密壳等

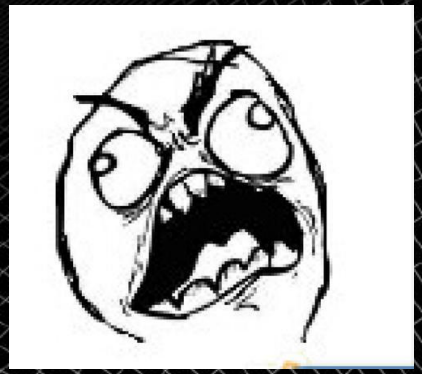
解题细节基础：编码解码、基础算法等

其他语言基础：安卓、IOS等

其他技能基础：堆栈结构、内存结构、数据结构、协议基础等



Pwn，在安全领域中指的是通过二进制/系统调用等方式获得目标主机的shell。CTF 中主要考察二进制漏洞的发掘和利用，需要对计算机操作系统底层有一定的了解。在 CTF 竞赛中，PWN 题目主要出现在 Linux 平台上。



CTF-PWN

- 一定是有漏洞的，可利用的。
- 基础好1小时大概率可完成该题目的破解

工作中的PWN

- 未知的漏洞
- 找个漏洞，未知时间

编程语言基础：C/C++、x86汇编、x64汇编、Python、ARM汇编等

操作系统基础：Linux内核基础、Windows内核基础

调试工具基础：IDA、Gdb、PwnTools等

安全漏洞基础：堆溢出、栈溢出、格式化字符串、ROP、Unlink、Uaf等

其他技能基础：（你底层会多少，学习起来速度就越快！）

CTF-MISC

- 一定是可解的题目
- MISC外号万能胶水，所有领域技术都可以粘合
- （比如PWN题里掺杂WEB等）

工作中的MISC

- 你1个人做10个安全攻城狮的任务
- （无法准确定义工作中的MISC，杂项：大杂烩）

多元化CTF-MISC-学习条件

- 流量分析：各种流量等
- 图片隐写：Exif、图像尾部、LSB等
- 文件雕修：Binwalk、DD、foremost、十六进制文本编辑器等
- 压缩文件：伪加密、CRC32爆破、已知明文攻击等
- 音频文件：莫尔斯、MP3、频谱隐写等
- 视频文件：MSU StegoVideo、Ffmpeg等
- 镜像分析：内存镜像等
- 其他基础：（互联网所有东西！）

没点数学基础都不玩

CTF-Crypto

- 一定是可解的题目
- 啥算法都可能是题目

工作中的Crypto

- 1个密码有可能怼5-10年
- 利用密码制作出独特的算法

- 古典密码：置换密码、栅栏密码、曲路密码、列位移密码等
- 替代密码：凯撒密码、维吉尼亚密码、希尔密码、Palyfair密码等
- 现代密码：对称密码、序列密码（AES）、公钥密码（RSA）等
- 哈希函数：MD5、SHA-1、SHA-512等
- 其他：消息认证码、消息认证码MAC、数字签名、标准数字DSA等
- 编程基础：C/C++、Python等

口算MD5?


攻防世界
World of Attack&Defense
答题
竞赛
排行榜
队伍
返回
返回选题
WEB
序号
1
001 view_source 1分 11375人
002 get_post 1分 9185人
003 robots 1分 9093人
004 backup 1分 8461人
007 simple_js 1分 6545人
008 xff_referer 1分 5754人
009 weak_auth 1分 6064人
010 webshell 1分 5772人

网络安全创新大会
Cyber Security Innovation Summit

目 录

CONTENTS

CTF 方向都玩一遍，选1个你最喜欢的、编程基础非常重要，选1个你最喜欢的
勿忘初心，时不时你要回到原点看下。

每个人学习兴奋的时候，元素点都不一样，如：

01 WEB-GetShell
PWN-GetShell

02 RE-第一次看懂汇编
WEB-第一次SQL注入

03 复现出黑客电影中的某个场景中的技术
通过某些事情有了很强大的存在感、自豪感

04 解决抵御电信诈骗
帮女盆友找回QQ

CTF+渗透学习攻略解析（兴奋剂元素寻找条件）

网络安全创新大会
Cyber Security Innovation Summit

寻找学习兴奋剂元素，需要环境的辅助，遇到反刺激成长时期更容易解放自我！（别挖过劲，注意把控）

场景一：家庭父母或亲戚反对你学计算机
场景二：你的亲戚就是做IT行业的，就是不帮你
场景三：你在学校成绩很差，根本没有存在感
场景四：老师根本不看好你，觉得你很渣渣
场景五：因为家庭条件报不起信息安全实地培训班
场景六：你CTF很牛逼，学校就是不支持你
场景七：你周围没有任何信息安全小伙伴或知音
场景八：患有游戏网瘾的你，找不到任何出路
场景九：自学安全拜师老被骗钱拉黑
场景十：学安全放弃了好几次，不知道原因

场景十一：老觉得自己不自信，自己不如人家
场景十二：觉得信息安全工资好高
场景十三：遇到问题，不断的想寻找答案
场景十四：黑客电影看多了，就是觉得牛逼
场景十五：中专老师的安全水平不如我
场景十六：我在的大学根本没有信息安全专业
场景十七：在网络里交流没人回答我问题，都是斗图
场景十八：我的家乡穷，不懂信息安全
场景十九：我周围的伙伴太牛逼，不敢吭声
场景二十：我就想给自己账号刷个VIP

先学漏洞，后学编程

先学编程，后学漏洞

我不学漏洞，不知道编程的重要性。因为我漏洞看不懂。我不学编程，不知道安全还能可以这么玩。还能挖掘出这么多漏洞！

你要牵引出兴趣，在看世界。世界都没兴趣看，还谈安全？

年轻的时候就应该摔摔打打练出来本事，因为你的资本就是年轻，你可以错误无数次。等你老了…

兴趣

兴趣是万物的根本

伙伴

如果不志同道合，你们交流都
不在1个次元，很难一起奔跑。

耐心

浮躁是正常的，学会弹性控制
千万不要持久的浮躁，要让
浮躁转化你为你的动力。

适应

你要适应成功和失败2个点，
在这2个点当中寻找1个平衡。

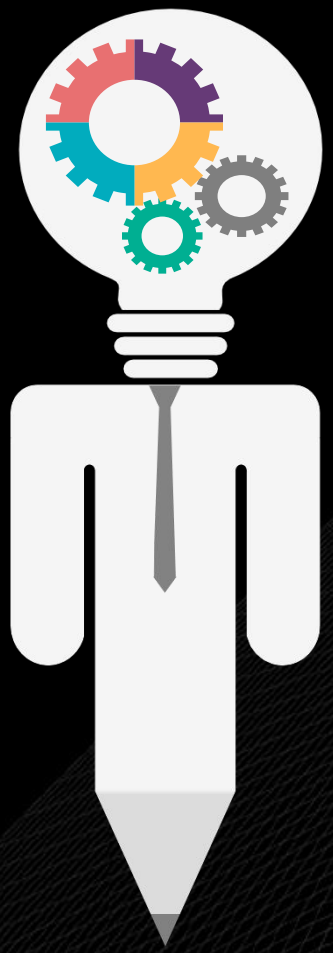
心态

不要老看人家牛逼，多看自己。
羡慕别人浪费时间，自我培养。

交流

别老当一个闷葫芦，容易憋坏。
多去互换心得体验，容易成长。

两点一线、三点一面、四点一体。



学会挖掘知识相互的异同点

如：20个编程语言里，思维是否相似？不同在哪？PWN、RE的题目共同的基础都需要哪些？

看文章与实战文章不在一个等级

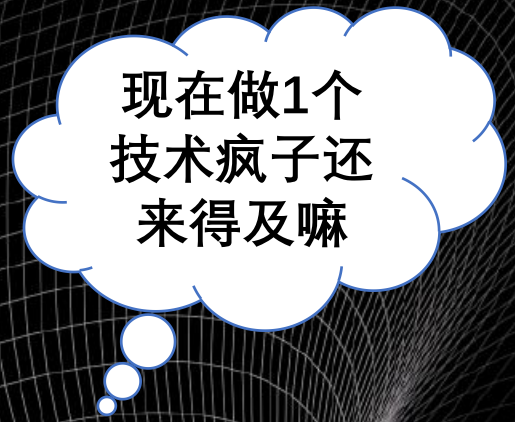
很多人下了教程感觉自己已经会了，很多人买了书籍没翻，感觉自己已经读懂了！

验证知识的拓展性和复用性

1个知识你学会了，是否可举一反三？是否可应用在其他场景下？是否真的可以万变不离其宗？

学会知识的归纳与总结

知识如果没有归纳、分类，到最终也不会总结出自己的东西。



你瞅啥

01 上学时期

叛逆：我TM就要辍学！
好处：提前接触社会去挣钱
风险：你做风险评估了嘛？

瞅你咋滴！

02 转行动机

忐忑：喜欢安全，转不转呢
好处：你做了你喜欢的事情
风险：你做风险评估了嘛？

导火索+契机

03 工作时期

不爽：我TM就要辞职！
好处：你可以拿到更高薪水
风险：你做风险评估了嘛？

再瞅一个试试

04 年龄危机

年龄：我过35了，来得及嘛
好处：你心态重新年轻1次
风险：你做风险评估了嘛？

试试就试试

K哥人生职业生涯心得笔记

No. 1

把控当前

你努力了，别人还是不认可。这是你控制不了的条件，你能控制的条件就是当前做好你自己。太在意别人的眼光容易迷失自己。

No. 2

玩出节奏

不要盲目追随他人的脚步，你要玩出自己的节奏，让你的节奏可任意嵌入1个群体当中。

No. 3

学会填坑

多解决实际问题，少一些抱怨，你会收获更多，否则你去下一个公司还是这个坑，你还是不会填。

1 没有一帆风顺，只有过关斩将

3 用汗水和时间打磨的东西会很价值

2 努力不一定成功，不努力一定不会成功

4 与其羡慕别人不如提升自己

Are You Ready?

金子是非常值钱的东西，如果你让自己变得非常像金子，那么请你想办法让光芒四射出去，让更多的人知道你是发光的。与其坐等别人识别你是个金子，不如你自己想办法让世界知道你是个金子！**学会自己创造东风！**自己动手，丰衣足食。


我就是安全技术菜死


装逼学
技巧与演
练
K哥，要不咱下去吧！
这会是不会有掌声的！
明年议题也没你的了！

网络安全创新大会
Cyber Security Innovation Summit

THANKS

姓名：孔韬循（K0r4dji@破晓团队）

公司：赛宁网安-攻防实验室

联系：admin@secbug.org