

知道创字研发技能表v3.0

2015/8/21 发布

by @知道创字(www.knownsec.com) @余弦 & 404团队

后续动态请关注微信公众号: **Lazy-Thought**

说明

关于知道创字

- 知行合一 | 守正出奇
- 知道创字是一家黑客文化浓厚的安全公司, 愿景是让互联网更好更安全

本技能表为知道创字研发工程师的技能树集合, 是的, 很庞大

- 聪明的人, 会根据每个tip自驱动扩展
- 不聪明的人, 坐等别人手把手, 不仅不适合知道创字, 也不适合任何有极客精神的公司

附件标志是我们推荐的附加资源, 感谢资源提供者

- [知道创字研发技能表v3.0离线版打包下载](#)

通用技能

公司与个人

- 公司是盈利性组织
- 个人和公司必须双赢
- 在认同公司理念且能够给公司创造足够价值的基础上, 为个人发展而工作

💡 WHO AM I

黑客是守正出奇且具备创造力的群体

守正出奇

- 这条正道/底线得坚守
- 但如果太过正就迂腐了, 为了搞定任务有时得出奇招

创造力

- 一个没有创造力的人是多么的可怜, 对于团队来说也是一种耻辱
- 本技能表的本质目的只有一个: 引导你拥有足够的创造力

- 黑客也可以是一种思维方式
- 我们需要对得起名片上的那个头衔: 工程师、研究员

牛人姿态

- 即使现在不是牛人, 也得具备这样的姿态
- 没有一定扎实内功与远见的人很少有这样的姿态
- 拥有不将就的做事风格, 迟早是牛人

如何做事

💡 方法论

- 完成一件事有好几条途径, 优秀的人的途径最短
- 任务拆分很容易得出做事的方法论

好的「方法论」会让你具备更强的「创造力」!


- 💡 时刻问自己: 「是否具备创造力?」

💡 任务拆分

- 成长过程会经历: 能力越大、责任越大、事情越多

思路

- 拆分细化为多个点

- 排好优先级
 - 任务四象限，决定优先级
 - 紧急重要
 - 赶紧搞定
 - 重要不紧急
 - 时刻持续关注，以免沦为「紧急重要」
 - 紧急不重要
 - 少少益善，学会拒绝
 - 不紧急不重要
 - 靠自律
 - SMART原则
 - S：任务是否明确
 - 不明确的任务搞起来就是浪费生命
 - M：任务是否可度量
 - 不可度量如何体现价值？
 - A：任务是否可搞定
 - 搞不定就不应该接，接就得有魄力搞定
 - R：任务的相关性如何
 - 决定了任务的价值，相关性越高越能体现价值，比如这个任务搞定了能让团队获得公司、客户等更大的认可
 - T：任务的时间
 - Timeline：任务时间轴，什么时间点需要搞定什么
 - Deadline：任务的最后期限，做评估时最好提前，因为总会有各种意外或拖延本性
 - Timeline上一些很关键的时间点我们可以称为里程碑，搞定每个里程碑应该庆祝下
 - 自己欠缺什么，立马发现
 - 是否需要寻求帮助，谁能帮你，自己单干？ 
 - 团队
 - 士气第一
 - 当你有团队时，分配与调度好任务很关键
 - 做得好是真并发
 - 做不好会死锁
- 沟通、反馈与责任
 - 一个无沟通能力的人，要么是天才，要么是不可爱的人，不过天才也就寥寥无几而已，你并不是
- 反馈要及时
 - 避免出问题不反馈，影响进度
- 方式
 - 正式的：邮件
 - 临时的：微信等即时通信
 - 着急的：给个电话
- 工作有大小，责任心无大小
- 周报的透明
 - 意义：大家互相了解工作与心得，有利于自己的判断与成长
 - 观察是一种多重要的技能

- 不是单纯的给领导汇报工作
- 周报需体现本周工作总结、下周工作计划、心得/问题/建议（我们叫唧唧歪歪）
- 周报可以很好体现一个人的
 - 总结能力
 - 计划能力
- 分享能力
 - 想象下：一个人从来没有心得/问题/建议的沉淀或反馈，这个人是一个相对封闭的人，在团队作战中很难达到默契
 - 当然，这种分享能力远不仅仅是在周报这种形式里

▫ 团队意识

- 很多人都说自己具备足够好的团队意识，但是有些人却并不是这样
 - 举个小例子：一个10人团队约定早上10点开会，而你迟到了10分钟，对于团队来说你浪费了整个团队100分钟（10人*10分钟）的生命。有些人无羞愧之心要么是意识不到这点，要么这个团队的风气就是这样...
- 团队意识是建立在互相信任的基础上
- Leader最关键，优秀的Leader一定会有个优秀团队
 - 兵熊熊一个
 - 将熊熊一窝
- 如何拥有个优秀的团队是一个复杂的话题

▫ 成长

- 新事物的敏感性
 - 保持好奇心
 - 不要局限在自己的圈子，适当跨界吸收灵感
 - 订阅国内外优秀博客/资源，深蓝阅读不错
 - 选择性参与一些必要的会议，听必要的主题，讨论必要的话题
- 💡 关于知识
 - 对知识的渴望程度决定了前进动力的大小
 - 当知识很廉价地摆在你面前，你反而不会珍惜
 - 对知识保持敬畏之心
- 不要让自己成为矫情/浮夸的人
- 和比你厉害的人在一起，和一流的人工作
 - 指点往往是精华
- ⚠️ 杜绝笨蛋爆炸
 - 二流的人招进来的人不太可能是一流的
 - 久而久之一个团队就笨蛋爆炸了
- 思考
 - 批判性思考
- 换位思考
 - 对于一个团队来说，这点太关键
- 💡 提问的智慧
 - 遇到问题先独立思考，尝试独立解决，尽最大努力后再提问
 - 提问时，礼貌很关键（对知识的敬畏），清晰表达很关键
 - 解决后，分享出来帮助更多需要帮助的人
- 💡 小事心态

- 越基础的事越关键，越需要细心
 - 不要一味盲目追求「高级感」，而忽视「小事」/「简单事」/「基础事」
 - 基础不牢、地动山摇
 - 小事做不好，别提大事
- ⚠️ 无论是个人还是团队的成长都需要不断沉淀知识，没有沉淀根基不稳

▢ ⚠️ 完成的定义

▢ 比如写个PoC

- 1. 搞懂了目标Web应用漏洞的原理
 - 2. 熟练运用Python各相关模块与机制
- ##### ▢ 3. 熟练了解了HTTP协议
- HTTP请求
 - HTTP响应
- 4. 代码写得够规范，让人看起来就是爽
- ##### ▢ 5. 程序经过足够的测试
- 黑测试
 - 白测试
- ##### ▢ 6. 及时反馈进度
- 我遇到困难了
 - 我搞定了
- 7. 更新相关文档，沉淀

▢ ⚠️ 熟练的定义

▢ 比如熟练SQL注入

- SQL语句这门“语言”能脱离文档顺手写出
- ##### ▢ 主流数据库的SQL特有函数、存储过程、机制我都了如指掌
- MySQL
 - MSSQL
 - Oracle
 - PostgreSQL
 - Access
 - SQLite
 - ...
- ##### ▢ 牛逼的工具我不仅用的顺其自然，源码还读过几遍，我能修改
- sqlmap
 - ...
- ##### ▢ 我具备创造性，而不仅仅是跟在大牛身后
- 研究出了几个不错的技巧
 - 发了几篇不错的Paper
 - 对外会议/沙龙等进行了几次分享
 - 写出了自己的相关工具，爽
- 我实战了N回，遇到了很多奇葩环境，我有足够的信心绕过
 - 以上这些之后，这才叫熟练！其他同理

▢ 好书推荐

▢ 推荐理由

- ##### ▢ 打通任督二脉的书，怎能不看？
- 但，尽信书不如无书

- 任何科学研究最终必须至少到哲学层面，触碰到上帝的脚
- 具体技术类书籍请见「专业技能」相关部分

☐ 鸡汤类

☐ 黑客与画家

☐ 印象深刻：设计者的品味

☐ 好设计是简单的设计

- 抓住本质

☐ 好设计是永不过时的设计

- 如果解决方法是丑陋的，那就肯定还有更好的解决方法，只是还没有发现而已

- 好设计是解决主要问题的设计
- 好设计是启发性的设计
- 好设计通常是有点趣味性的设计
- 好设计是艰苦的设计
- 好设计是看似容易的设计
- 好设计是对称的设计
- 好设计是模仿大自然的设计
- 好设计是一种再设计
- 好设计是能够复制的设计
- 好设计往往是奇特的设计
- 好设计是成批出现的
- 好设计常常是大胆的设计

☐ 浪潮之巅

- 感受IT帝国的崛起与没落，我们现在站在又一个互联网浪潮之巅

☐ 洁癖类

- 重构
- 代码整洁之道
- 代码大全2

☐ 敏捷类

☐ Rework中文版

- 37signals团队的敏捷经验
- 高效程序员的45个习惯

☐ 产品类

- 人人都是产品经理
- 结网

☐ 神书

- 自私的基因
- 失控

- ...

☐ 专业技能

☐ 💡 原则

- 至少完整看完与练习好一本书
- 至少过一遍官方文档

☐ ★ 基础必备

☐ HTTP抓包与调试

- ▣ Firefox插件
 - ▣ Firebug
 - 抓包与各种调试
 - ▣ Tamper Data
 - 拦截修改
 - ▣ Live Http Header
 - 重放功能
 - ▣ Hackbar
 - 编码解码/POST提交
 - ▣ Modify Headers
 - 修改头部
- ▣ Fiddler
 - 浏览器代理神器
 - 拦截请求或响应
 - 抓包
 - 重放
 - 模拟请求
 - 编码解码
- ▣ 第三方扩展
 - ▣ Watcher
 - Web前端安全的自动审计工具
- ▣ Wireshark
 - 各种强大的过滤器语法
- ▣ Tcpdump
 - 命令行的类Wireshark抓包神器
- ▣ Python
 - ▣ urllib2
 - ▣ 打开请求响应调试
 - 编辑urllib2的do_open里的h.set_debuglevel
 - 改为h.set_debuglevel(1)，这时可以清晰看到请求响应数据，包括https
- ▣ 什么是跳转
 - ▣ 服务端跳转
 - ▣ 302
 - <?php header("Location: 3.php"); ?>
 - ▣ 301
 - <?php header("HTTP/1.1 301 Moved Permanently"); header("Location: 2.php"); ?>
 - ▣ u=urllib2.urlopen(url)后，u.url能得到服务端跳转后的地址
 - urllib2自己的特性
 - 所谓的会跟进去
- ▣ 客户端跳转
 - ▣ <meta http-equiv="refresh" content="0; url=http://www.evilcos.me" />
 - htmlparse解析就行了
 - ▣ location.href="http://" + "/evilcos.me";
 - 正则解析（弱）
 - JavaScript引擎解析（强）

- ☐ Office能力
 - Word文档编写，看去要专业，尤其对外的
 - Excel里面大量的统计、图表功能，需要善于使用
 - PPT演讲、培训等必备，如何做好PPT？ 百度一下...
- ☐ 😊 进一步
 - yEd
 - Visio
 - ☐ FreeMind
 - 本技能表就是这个制作
- ☐ 上手Linux
 - 《鸟哥的Linux私房菜》
- ☐ 熟练VIM
 - 实战至少3回合： <http://coolshell.cn/articles/5426.html> 
- ☐ 上手Python
 - 💡 <https://www.python.org/dev/peps/pep-0008/> 
 - 💡 <http://learnpythonthehardway.org/book/> 
- ☐ 《Python核心编程2》
 - ☐ 第4章 Python对象
 - 完整熟练
 - ☐ 6.8 Unicode
 - 完整熟练
 - ☐ 8.11 迭代器和iter()函数
 - 完整熟练
 - ☐ 第9章 文件的输入和输出
 - 完整熟练
 - ☐ 第10章 错误和异常
 - 完整熟练
 - ☐ 第11章 函数和函数式编程
 - 完整熟练
 - ☐ 第12章 模块
 - 完整熟练
 - ☐ 第14章 执行环境
 - 完整熟练
 - ☐ 第15章 正则表达式
 - 💡 完整熟练
 - ☐ 第18章 多线程编程
 - 完整熟练
 - ☐ 20.2 使用Python进行Web应用：创建一个简单的Web客户端
 - 完整熟练
- ☐ 算法
 - 快排
 - 二分
- ☐ 正则表达式
 - ☐ 调试工具

- 🤖 Kodos
- 💡 RegexBuddy
 - 支持多种语言
 - 支持调试优化
- 😊 <http://www.regexper.com/> 
 - 正则图解
- 正则表达式30分钟入门教程: <http://deerchao.net/tutorials/regex/regex.htm> 
- <http://wiki.ubuntu.org.cn/Python正则表达式操作指南> 
- 《精通正则表达式》
- 研发能力
 - 瀑布模型
 - 需求->需求分析->设计->开发->测试->上线->运维/运营
 - 💡 需求分析能力
 - 给你一个需求, 如何给出一个优美的执行思路——方法论
 - 这个能力非常非常非常的关键
 - 调试能力
 - 只要定位出, 就没有解决不了的Bugs
 - 肉眼看到的都是假象
 - 一定要专业的工具与经验配合
 - Bugs在哪出现, 最终就在哪进行真实模拟调试
 - 缩小范围
 - 构建自己的测试样例
 - 排除网络复杂未知情况
 - 关联模块一个个排除
 - Python单步调试
 - `import pdb;pdb.set_trace()`
 - 在需要单步调试的地方加上面这句, 运行程序后中断在此, 然后查看指令进行一步步细细调试
 - 粗暴调试: `print`
 - 敏捷思想
 - 快速迭代
 - 任务拆细
 - 💡 v1原则: 定义好v1的目标, 快速完成v1为优先
 - 习惯Wiki记录, 利于沉淀与分享
- 翻墙
 - 优雅解决方案
 - shadowsocks + 一台海外 VPS + Chrome(SwitchyOmega)/Firefox(AutoProxy)
 - 详情了解: http://mp.weixin.qq.com/s?__biz=MzA3NTEzMTUwNA==&mid=210457700&idx=1&sn=322d1e4c13d3f33ade848e3889c410b 
 - SSH隧道
 - <http://www.ibm.com/developerworks/cn/linux/l-cn-sshforward/index.html> 
 - 本地转发
 - `ssh -L <local port>:<remote host>:<remote port> <SSH hostname>`

- 远程转发
 - 反弹
 - `ssh -R <local port>:<remote host>:<remote port> <SSH hostname>`
- 动态转发
 - `ssh -D <local port> <SSH Server>`

▫ Web安全

▫ 零基础如何学习Web安全

- <http://www.zhihu.com/question/21606800/answer/22268855> 

▫ Web服务组件

- 8+1：一图胜千言哎:) 

▫ 钟馗之眼

- 网络空间搜索引擎
- <http://zoomeye.org> 
- 大量样例：<http://www.zoomeye.org/search/dork> 

- 组件具有影响面，越底层的组件影响面可能越大

▫ 安全维度

- 漏洞
- 风险
- 事件

▫ Web安全标准

- OWASP
- WASC

▫ 实战环境

▫ XSS

▫ 内部平台：ks-xsslab_open

▫ 可以上手

- XSS
- CSRF
- ClickJacking

▫ <http://xss-quiz.int21h.jp/>

-  答案：[xss_quiz.txt](#) 

▫ <http://prompt.ml/0>

- 答案：<https://github.com/cure53/XSSChallengeWiki/wiki/prompt.ml> 

▫ <http://escape.alf.nu/>

- 答案：<http://blog.nsfocus.net/alert1-to-win-write-up/> 

▫ SQL



▫ <https://github.com/Audi-1/sqli-labs>

- SQLI-LABS is a platform to learn SQLI

▫ i春秋





- <http://www.ichunqiu.com/> 

▫ Sebug + ZoomEye

- <http://sebug.net> 
- <http://zoomeye.org> 
- 你懂得...

▫ 工具

▫ 我的渗透利器


- ☐ Firefox
 - ☐ Firebug
 - 调试JavaScript, HTTP请求响应观察, Cookie, DOM树观察等
 - ☐ Tamper Data
 - 拦截修改
 - ☐ Live Http Header
 - 重放功能
 - ☐ Hackbar
 - 编码解码/POST提交
 - ☐ Modify Headers
 - 修改头部
 - ☐ GreaseMonkey
 - [Original Cookie Injector for Greasemonkey](#) 
 - ☐ NoScript
 - 进行一些JavaScript的阻断
 - ☐ AutoProxy
 - 翻墙必备
- ☐ Chrome
 - ☐ F12
 - 打开开发者工具, 功能==Firebug+本地存储观察等
 - ☐ SwichySharp
 - 翻墙必备
 - ☐ CookieHacker
 - <http://evilcos.me/?p=366> 
- ☐ Web2.0 Hacking
 - ☐ XSS'OR
 - 常用其中加解密与代码生成
 - <http://evilcos.me/lab/xssor/> 
 - 源码: <https://github.com/evilcos/xssor> 
 - ☐ XSSEE 3.0 Beta
 - Monyer开发的, 加解密最好用神器
 - <http://evilcos.me/lab/xssee/> 
 - ☐ Online JavaScript beautifier
 - JavaScript美化工具, 分析JavaScript常用
 - <http://jsbeautifier.org/> 
 - ☐ BeEF
 - The Browser Exploitation Framework
 - <http://beefproject.com/> 
- ☐ HTTP代理
 - ☐ Fiddler
 - 非常经典好用的Web调试代理工具
 - ☐ Burp Suite
 - 神器, 不仅HTTP代理, 还有爬虫、漏洞扫描、渗透、爆破等功能
 - ☐ mitmproxy
 - Python写的, 基于这个框架写神器实在太方便了
- ☐ 漏洞扫描

- ▣ AWVS
 - 不仅漏扫方便，自带的一些小工具也好用
- ▣ Nmap
 - 绝对不仅仅是端口扫描！几百个脚本
 - Python自写脚本/工具
- ▣ 漏洞利用
 - ▣ sqlmap
 - SQL注入利用最牛神器，没有之一
 - ▣ Metasploit
 - 最经典的渗透框架
 - ▣ Hydra
 - 爆破必备
- ▣ 抓包工具
 - ▣ Wireshark
 - 抓包必备
 - ▣ Tcpdump
 - Linux下命令行抓包，结果可以给Wireshark分析
- ▣ Sebug + ZoomEye
 - 类似这类平台都是我们需要的
 - ▣ Sebug类似的
 - <https://www.exploit-db.com/>
 - ▣ ZoomEye类似的
 - <https://www.shodan.io/>
- ▣ Kali Linux
 - 除了上面介绍的一些工具，其他海量各类型黑客工具，自己去摸索

▣ 书

- 《黑客攻防技术宝典（Web实战篇）》
- 《白帽子讲Web安全》
- ▣ 《Web前端黑客技术揭秘》
 - 我和xisigr出品
- 《Web之困》
- 《SQL注入攻击与防御》

▣ papers









- <http://www.exploit-db.com/papers/> 
- BlackHat/Defcon/XCon/KCon/国内各安全沙龙等相关Papers需要持续跟进

▣ 嵌入式安全

▣ 路由器安全

▣ 基础

- 嵌入式Linux系统方面知识
- 开发系统互联参考模型-第三层网络层
- MIPS/ARM汇编知识
- VxWorks系统方面知识
- JTAG调试接口规范
- 嵌入式系统交叉环境开发

- 路由器芯片方案提供商
 - 博通
 - Atheros
 - TrendChip
 - ACROSPEED
 - IC+
 - 瑞昱
 - ...
- 站点
 - <https://www.openwrt.org/> 
 - OpenWrt is described as a Linux distribution for embedded devices
 - <http://routerpwn.com> 
 - 全球主流路由器相关漏洞大集合
 - http://see.sl088.com/wiki/Uboot_%E7%BC%96%E8%AF%91 
 - Uboot_编译
 - <http://www.devtty0.com/> 
 - Embedded Device Hacking
- 工具
 - Binwalk
 - IDA Pro
 - gdb/gdbserver
 - qemu-system
 - qemu-user-static
 - Smiasm
 - Metasm
 - JTAG硬件调试器
- 书
 - 《揭秘家用路由器0day漏洞挖掘技术》
 - 《Hacking the XBOX: An Introduction to Reverse Engineering》
 - 《Hacking the Cable Modem: What Cable Companies Don't Want You to Know》
 - 《MIPS体系结构透视 》
 - 《计算机组成与设计：硬件、软件接口》
- 摄像头安全
 - <http://www.openipcam.com/> 
 - <https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf> 
- 工控安全
 - 基础
 - 工业生产环境的基本结构，如：SCADA、PCS
 - 工业生产环境的信息安全风险点（可参考DHS出版物）
 - Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
 - 工控网络组态、逻辑开发、应用组态的基本技术方法
 - 抓包、看RFC分析几个常规工业以太网协议，如：Profinet、Modbus
 - 买两款PLC玩玩，会真实感受到工业环境的信息安全问题（一定记得买以太网模块，不贵二手几百块）
- 站点
 - 事件跟踪分析
 - <http://plcscan.org/blog/> 
 - <http://scadastrangelove.blogspot.kr> 

- <http://www.phdays.com/>
- <http://www.scadasl.org>
- <https://scadahacker.com>
 - Duqu
 - <https://scadahacker.com/resources/duqu.html>
 - Stuxnet
 - <https://scadahacker.com/resources/stuxnet.html>
 - Havex
 - <https://scadahacker.com/resources/havex.html>
- 标准协会/测试工具
 - DHS CET套件
 - <http://ics-cert.us-cert.gov/Assessments>
 - NERC ES-ISAC
 - <http://www.esisac.com/SitePages/Home.aspx>
 - ICS-ISAC
 - <http://ics-isac.org>
 - NTSB美国国家工控测试床
 - <http://energy.gov/oe/downloads/common-cyber-security-vulnerabilitiesobserved-control-system-assessments-inl-nstb>
 - NIST SP 800-82
 - <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
 - ISA-99控制系统安全协会
 - <http://isa99.isa.org/ISA99%20Wiki/Home.aspx>
 - NERC CIP标准
 - <http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx>
- 工具
 - 仿真类
 - 电力仿真软件testhaness
 - Modbus仿真软件ModScan
 - 电力104协议仿真软件PMA
 - 测试类
 - Wurldtech Achilles
 - Codenomicon Defensics
 - Spirent
 - BPS
 - 源代码
 - 发现
 - <https://code.google.com/p/plcscan/>
 - <https://code.google.com/p/modscan/>
 - <https://github.com/arnaudsoullie/scan7>
 - <https://github.com/atimorin>
 - <https://github.com/digitalbond/Redpoint>
 - 操纵
 - <https://www.scadaforce.com/modbus>
 - <https://github.com/bashwork/pymodbus>
 - <https://rubygems.org/gems/modbus-cli>
 - <http://libnodave.sourceforge.net>
 - <https://code.google.com/p/dnp3>

- 异常监测
 - <http://blog.snort.org/2012/01/snort-292-scada-preprocessors.html> 
 - <http://www.digitalbond.com/tools/quickdraw/> 
- Fuzz
 - <https://github.com/jseidl/peach-pit/blob/master/modbus/modbus.xml> 
- 其他
 - ZoomEye工控专题: <http://ics.zoomeye.org/> 
 - Shodan工控专题: <https://www.shodan.io/report/l7VjfVKc> 
 - <https://github.com/evilcos/papers/blob/master/网络空间工控设备的发现与入侵.ppt> 
- zoomeye.org
 - 全球可以找到无数真实路由器/摄像头/工控设备等
 - 如: <http://www.zoomeye.org/search?q=app:%22MikroTik%20RouterOS%22&from=dork> 
- 研发清单
 - 编码环境
 - pip
 - Vagrant
 - tmux/screen
 - vim
 - Markdown
 - zsh + oh-my-zsh
 - Python2.7
 - >Django1.4
 - <http://djangobook.py3k.cn/2.0/> 
 - Django Debug Toolbar 
 - 其他框架
 - web.py
 - Flask
 - Tornado
 - node.js
 - Ubuntu/Gentoo/Centos
 - ipython
 - 版本控制
 - 废弃SVN, 全面拥抱Git
 - GitLab
 - Nginx+uWSGI
- Python
 - 官方手册
 - 至少过一遍, 这都没过一遍, 视野会局限
 - 行之说: 「我没看过Python的书, 却熟读官方手册...」
- Linux/UNIX
 - 书
 - 《鸟哥的Linux私房菜》
 - 《Linux Shell脚本攻略》
 - 《UNIX编程艺术》
 - 《Software Design 中文版 01》 《Software Design 中文版 02》 《Software Design 中文版 03》
 - 让你的电脑默认操作系统就是Linux...
- 前端

- 书
 - 《JavaScript DOM编程艺术》
- 了解DOM
 - 这同样是搞好前端安全的必要基础
- 库
 - jQuery
 - 优秀的插件应该体验一遍，并做些尝试
 - 官方文档得过一遍
 - D3.js
 - ECharts
 - 来自百度
 - Google API
 - ZoomEye Map组件
 - ZoomEye团队自己基于开源的打造
 - AngularJS
 - Google出品的颠覆性前端框架
 - Bootstrap
 - 应该使用一遍
- 爬虫进阶
 - 代理池
 - 爬虫「稳定」需要
 - 网络请求
 - wget/curl
 - urllib2/httpplib2/requests
 - 💡 scrapy
 - 验证码破解
 - pytesser
- 调度
 - crontab是最原生的定时调度
 - 基于redis实现的分布式调度
 - 基于rpyc实现的分布式调度
 - celery/gearman等调度框架
- 并发
 - 线程池
 - 进程内优美的并发方案
 - 协程
 - 进程内另一种优美的并发方案
 - gevent
 - 多进程
 - os.fork
 - 💡 multiprocessing
- 数据结构
 - JSON
 - cPickle
 - protobuf

▣ 数据存储及处理

▣ 数据库

- MySQL
- MongoDB
- Cassandra
- Hadoop体系
- Redis
- Sqlite
- bsddb
- ElasticSearch

▣ 大数据处理

- Hive
- Spark


▣ ELK

- ElasticSearch
- Logstash
- Kibana

▣ DevOps

- SSH证书
- Fabric
- SaltStack
- puppet
- pssh/dsh

▣ 运维进阶

- 运维工程师必须掌握的基础技能有哪些?
- <http://www.zhihu.com/question/23665108/answer/25299881> 

▣ 调试

- pdb
- logging
- Sentry
- strace/ltrace
- lsof

▣ 性能

▣ Python内

- timeit
- cProfile
- Python性能分析指南: <http://www.oschina.net/translate/python-performance-analysis> 

▣ Python外

- top/htop/free/iostat/vmstat/ifconfig/iftop...

▣ 算法

- 分词
- 贝叶斯
- 神经元
- 遗传算法
- 聚类/分类
- ...

▣ 持续集成

▣ 自测试

- nose

- Jenkins

☐ 安全

☐ 我的分享

- 程序员与黑客: <http://www.infoq.com/cn/presentations/programmers-and-hackers> 



☐ 协作

- 类似Trello的在线协同平台
- Slack
- 微信
- 立会

☐ 设计思想

- 人人都是架构师: 具备架构思想是一件多酷的事
- 实战出真知

☐ 如何设计

-  [任务架构设计变迁.pdf](#) 
- 松耦合、紧内聚
- 单元与单元属性
- 生产者与消费者

☐ 结构

- 队列
- LRU

☐ 分布式

- 存储
- 计算

☐ 资源考虑

- CPU
- 内存
- 带宽

☐ 粗暴美学/暴力美学

- 大数据, 先考虑run it, 然后才能知道规律在哪
- 「run it优先」能快速打通整体, 洞察问题
- 「run it优先」能摆脱细节(繁枝末节)的束缚
- 「run it优先」能快速迭代出伟大的v1

☐ 一个字总结

- 美

☐ 牛人1,2,3

- 1研究: 研究东西, 有足够洞察力, 研究水准不错
- 2研发: Hack Idea自己有魄力实现, 不懂研发的黑客如同不会游泳的海盗
- 3工程: 研发出来的需要实战、需要工程化, 否则只是玩具, 而不能成为真的武器

☐ 优质资源

☐ 书

- 多关注电子工业/图灵/机械工业/人民邮电等出版社, 他们有专业团队来保障每年输出优质书籍
- 自己需要掌握鉴别好书的能力

☐ 站点

- 知乎周刊: <http://zhuanlan.zhihu.com/Weekly> 
- 码农周刊: <http://weekly.manong.io/> 
- Pycoder's Weekly: <http://pycoders.com/archive/> 
- Hacker News: <https://news.ycombinator.com/> 

- Startup News: <http://news.dbanotes.net/> 
- 开发者头条: <http://toutiao.io/> 
- 极客头条: <http://geek.csdn.net/> 
- InfoQ: <http://www.infoq.com/cn> 
- Stack Overflow: <http://stackoverflow.com/> 
- GitHub: <https://github.com/> 
- FreeBuf: <http://www.freebuf.com/> 
- WooYun: <http://drops.wooyun.org/> 
- 深蓝阅读: <http://bluereader.org/> 

▣ RSS订阅


▣ 漏洞相关

- <http://sebug.net/rss.xml> 
- <https://www.exploit-db.com/rss.xml> 
- <https://rss.packetstormsecurity.com> 
- <http://www.wooyun.org/feeds/public> 

▣ 强烈推荐圈内人打造的深蓝阅读

- <http://bluereader.org/> 
- 这上面已经很多黑客/技术类似的RSS资源了

▣ 威胁情报


- 本来不想提任何这方面的，想想还是抖个资源，如下
- <https://github.com/kbandla/APTnotes> 

▣ 安全平台

▣ 在线学习平台

- i春秋: <http://www.ichunqiu.com> 
- <https://pentesterlab.com> 

▣ PoC提交与学习

- Sebug: <http://sebug.net> 
- Beebeeto: <http://www.beebeeto.com> 
- Bugscan: <http://www.bugscan.net> 
- Tangscan: <http://www.tangscan.com> 

▣ 结尾

- 本技能表会持续不断更新
- 如果有相关好资源/建议可以联系我: evilcos@gmail.com
- ▣ 如果本技能表引起你的强烈共鸣，想加入我们，可以联系我: evilcos@gmail.com，我会结合你的情况
 - 给你仅仅一道有趣的笔试题
 - 或者和你线下约聊
- ⚠ 邮件联系我，邮件标题务必包含「技能表」三个字，感谢
- **TO BE A HACKER:)**