《K哥谈：白帽子转型养成之路》

孔韬循（K0r4dji）| 北京丁牛科技有限公司-首席安全官（CSO）

个人简介

姓名籍贯：孔韬循，籍贯内蒙古-赤峰市，93年，网络ID：K0r4dji（小K）

项目经验：拥有多年国家级党政军信息安全服务经验

接触时间：2008年左右接触（15-16岁期间）

所在职位：北京丁牛科技有限公司-首席安全官（CSO）

安全团队：国内信息安全研究团队-破晓团队（Pox Team）创始人

个人名言：没有高手和菜鸟，只有玩的多和少！

相关书籍：

1.中国工信出版集团-电子工业出版社《Web安全深度剖析》原稿审核/修改人

2.中国工信出版集团-电子工业出版社《Python带我起飞》专家书评撰写人

3.中国工信出版集团-人民邮电出版社《Windows黑客编程技术详解》专家书评撰写人

.....

个人简介-其他信息

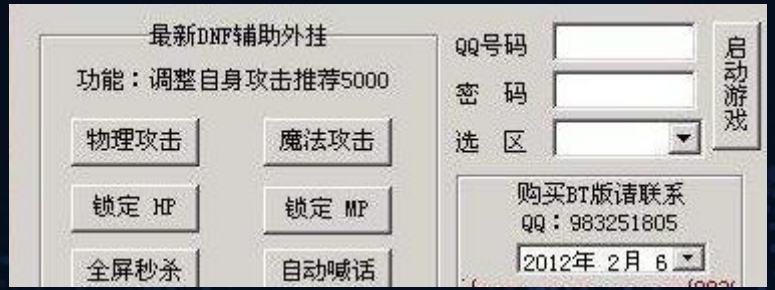
- 1.中央企业-中国电子CEC-可信华泰教育事业-技术专家顾问
- 2.中国工信出版集团-人民邮电出版社-IT专业图书专家顾问
- 3.中国Python开发者大会-特邀讲师
- 4.国家教育部-第九届全国大学生信息安全竞赛-嘉宾/评委
- 5.广州大学-网络信息安全CTF夏令营-方滨兴院士班-高级讲师
- 6.赛宁网安-白帽子学院-资深专家顾问（院长：诸葛建伟）
- 7.北京蓝森科技-15PB二进制安全实地培训机构-特邀讲师
- ....

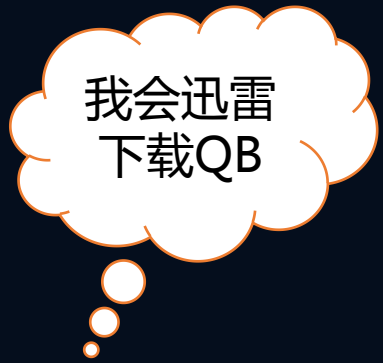
FIT 2019

目录

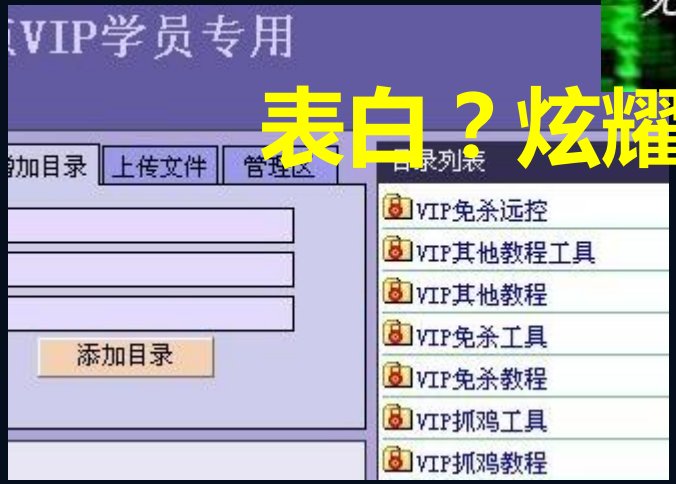
虚拟世界财产被盗取

游戏账号：大话西游/热血江湖/梦幻西游/天龙八部/CF穿越火线/DNF地下城与勇士...
社交账号：QQ
....





拜师收徒，只要8.8，寒暑假冲刺班



表白？炫耀？虚荣？装X？...

赶紧组建团队开始搞事情

招人：XX负责人、XX导师、XX讲师、

开班：WebShell提权班、渗透班、DDOS抓鸡班、免杀班、编程班、外挂辅助班....

名字：中国XX家族、中国XX黑客联盟、中国XX小组、中国XX安全团队...

搞事：Hacker By Helen（梗）、教父-郭某华、此站/此号/此群被社....

惹事：你很牛逼嘛？求社！求D！ 我大哥是XX，不服你来打我！....（调侃）

年轻气盛，希望最后能有真正意义的成长与发展！

看眼眼熟的工具....


旁注WEB综合检测程序 Ver3.6修正版 (09.10.14版) [黑客动画吧出品 - 明小子]
旁注检测
综合上传
SQL注入
PHP注入
数据库管理
破解工具
辅助工具
关于程序
批量扫描注入点
SQL注入猜解检测
MSSQL辅助工具
管理入口扫描
检测设置区
该板块功能介绍
设置
载入查询网址
添加网址
载入二级域名
导入网址
检测:
批量分析注入点
20个线程
连接地址:共368条
http://www. com/./new.asp?tid=3
http://www. com/./new.asp?tid=5
http://www. com/news.asp?newsid=1359
http://www. com/list.asp?anclassid=47
相关工具
设置选项
关于...

看眼眼熟的工具....


PEiD v0.94
文件: D:\需要
入口点:
文件偏移:
连接器版本:
ASPack 2.12
多文件扫描
总在最前
ImportRE
c:\documents a
rva:00055
rva:00055
rva:00055
rva:00055
rva:00055
rva:00055
rva:00055
rva:00055
rva:000552F0
当前的输入信息:
D (十进制:13) 有
171 (十进制:369)
(2 (十进制:2) 未
IAT
OEP 0005159C
RVA 00055128
载入树文件
保存树文件
获得输入信息
EXE捆绑机
[捆绑文件]
开始捆绑第一个可执行文件与第二个可执行文件，生成捆绑后的文件。
点击这里 开始
EXE捆绑机
捆绑文件成功!
确定
要退出，请点击“取消”。
< 上一步(B)
下一步(N) >
取消
修理抓取文件
结束位置 132
添加已确定特征码范围

看眼眼熟的工具....


花刺代理验证 (P
Cheat Engine 5.6.1
文件(F) 编辑(E) 进程(P) 帮助(H)
00001454-Lingoes.exe
找到: 1,905
地址 值
新的扫描
再次扫描
撤消扫描
设置
数值:
Hex 11
扫描类型 精确值
数值类型 4 个字节
内存扫描选项
用户模式
所有
从
到
00000000
7FFFFFFF
显示
禁止随机
启用速度修改
同时扫描只读内存
快速扫描
深层扫描
在扫描时暂停游戏
查看内存
手动添加地址
锁定 说明 地址 类型 数值
SQLTOO
SQL连接
IP地址
上传步骤
本地文件
SHELL
DOS 命令
命令 :
恢复
DLL路径
台湾
上海
西藏
湖北
中国代理2

眼熟的课程...

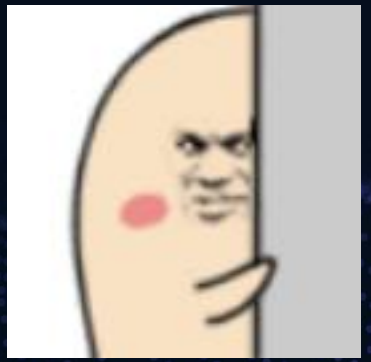
- 饭客黑客之免杀教程
- 饭客黑客之入侵教程.
- 饭客黑客之基础教程.
- 饭客黑客之提权教程.
- 饭客黑客之网赚教程.
- 饭客黑客之脱壳破解

- 黑客基地软件破解特训班1-19.rar
- 黑客基地软件破解特训班20-38.rar
- 黑鹰破解教程.iso
- 甲壳虫脱壳破解班.rar
- 中华隐士黑客联盟软件破解及解密系列

- YES黑客联盟初级免杀培训教程.rar
- 暗组Gh0st编译免杀系列教程.rar
- 暗组免杀教程.rar
- 饭客Gh0st源码免杀VIP教程.rar
- 红色黑客联盟免杀教程.rar
- 华中红客基地菜鸟学习MianS系列教程.rar
- 小七VIP_2013年无特征高级技巧处理(主要
- 新世纪网安VIP高级免杀班1-16.rar
- 新世纪网安VIP高级免杀班17-31.rar
- 夜鹰海盗盟初级免杀培训教程.rar

- 冰客安全网渗透系列.rar
- 饭客脚本入侵.rar
- 黑客动画吧Web入侵班1-16.rar
- 黑客动画吧Web入侵班17-31.rar
- 黑客动画吧之网易学院新手脚本系列
- 黑客防线2009脚本课程.rar
- 红黑脚本攻防20课全.rar
- 华夏入侵.rar
- 华中红客入侵.rar

一个没学会



不是我们太年轻，而是没有人愿意正确引导

FIT 2019

引导不足

不用搭理他们，都是小学生

诱惑四起

老板日站嘛，1个10万

肆无忌惮

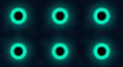
无所谓，别人入侵我看也没事，我也不能有啥事情

根深蒂固

你不GetShell提权拿服务器脱裤，还学什么网络安全？

FIT 2019

目录



目前的状态，CTF+刷漏洞平台

XCTF 国际网络攻防联赛

哪个师傅带带我？

知守 ZHISHOU · CSC

IT技能充电-培训方式补充营养

FIT 2019

- 1.现在的渗透跟以前不一样了
- 2.现在的二进制也跟以前不一样了
- 3.现在的公司企业岗位需求跟以前不一样了
- 4.现在的求职门槛也不一样了
- 5.现在的技术门槛跟以前也不一样了

15PB 十五派信息安全教育 15PB Information Security Education

LanQu 蓝鸥

XDL 兄弟连教育 www.itxdl.cn

安全牛 AQNIU.COM

春秋

合天智汇

目前的心理活动

初级(0-1)

- 拜师学艺
- 八方看看
- 结实伙伴

中级(2-4)

- 技艺实战
- 四处游荡
- 团队组建

高级(5-8)

- 技艺娴熟
- 目标锁定
- 团队发展

优秀

白帽子内心弹幕墙！

FIT 2019

你厉害你牛逼

这个人绝对是大佬

一群SB

这个小姐姐好漂酿

呵呵

都是大佬

他还不如我呢

这哥们技术屌的一匹

凭啥他就比我牛逼

我要当大佬

我就是不服

去哪找个工作呢

好像不适合做安全哎..

SRC坑爹

漏洞审核SB

我就鄙视你了咋地吧

我娱乐圈了咋地吧

不服你咬我啊

白帽子团队-破晓团队（Pox Team）

灵魂创建：2013年10月，2014年中旬开始运营
团队文化：路虽远，行则必达。事虽难，做则必成！
官方网站：http://www.SecBug.org
团队人数：60-70人
成员组合：CETC中国网安、腾讯安全应急响应中心、美图秀秀、联想、安天、安恒、国家电网-电力科学研究院、中国电子、德国电信、银行、中国农科院、360集团、360企业安全集团、启明星辰ADLAB实验室、天融信阿尔法实验室、知道创宇、T00ls多板块/多位版主、Python开发者组委会核心、中国石油、国家队...等，安全研究经验3-20年不等。
相关书籍：《Web安全深度剖析》/《Python带我起飞》/《Windows黑客编程技术详解》
团队日常：SRC漏洞/书籍编写/技术切磋/心情分享/CTF/职位内推/活动合作/企业辅助...等
成员职位：工程师->组长->经理->总监->首席安全官->CEO首席执行官...阶段不等。
行业贡献：人才输送、人才中转、人才培养、课程分享、文章分享、其他扶持...等
组建意义：让大家有归属感，有喜欢的事情自由研究并实现出来，分享更多的事物。

理念：SRC/CTF刷的再牛逼，有困难了不去帮忙，这支队伍的灵魂是有问题的！

如何做好一名白帽子？

白帽子-DM：在遵守法律的前提下，对安全知识能做到刨根问底，追求理论和实战相结合，不拘泥于工具的使用。要有一门自己很熟练的编程语言，把自己的想法付诸于行动，用代码实现它。肯花时间去钻研，不要把时间浪费在没有意义的事上。作家格拉德威尔说过：要成为某个领域的专家，需要10000小时，按比例计算就是：如果每天工作八个小时，一周工作五天，那么成为一个领域的专家至少需要五年。自己对一个事物的认知程度取决于自己对这个事物花了多少时间。当然前提是这个时间是属于有效时间。

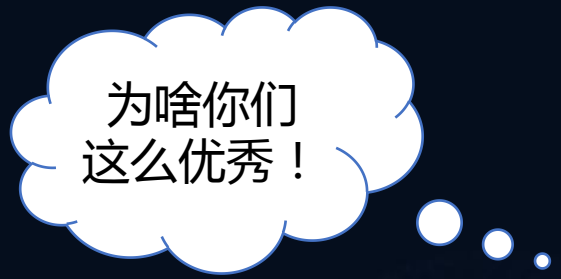
白帽子-岩少：做自己该做的事情，接自己力所能及的东西，坚决不能触碰红线。

白帽子-Simple：保持激情上进的态度，不断探索学习新兴技术，实践多于理论。

如何做好一名白帽子？

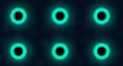
白帽子-红客十年：首先我们要了解白帽子存在的意义，只有了解了白帽子存在的意义，才能去做好白帽子，白帽子是一个黑灰产业时代诞生出的新生群体，这个群体的存在是为了守护安全，但现在在利益的驱使下和圈子文化的感染下，已经没有纯粹的白帽子了，我们应该属于这个安全时代的先驱者，看到身边很多朋友都在利益和圈子文化里沉下去了，希望后起的白帽子要记住你成为白帽子的初心是什么，不要跟着利益和圈子文化去改变自己，要做到真正的不忘初心！

白帽子-Saviour：Emmm.....

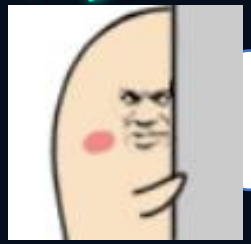


FIT 2019

目录



未来发展与规划-生活与学习



取个媳妇生个娃，老婆孩子热炕头

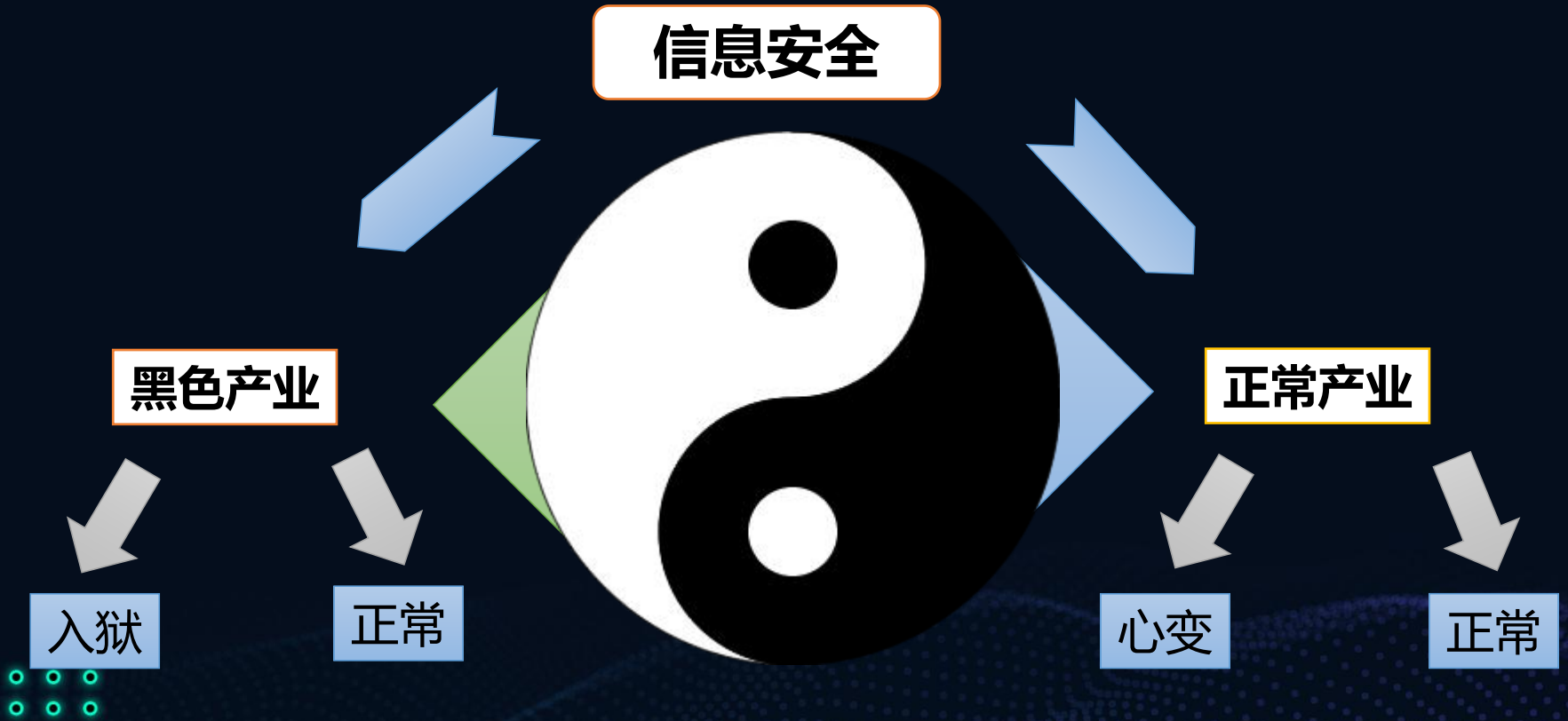
我要买一个大房子

我要把某个领域的技术学的很得心应手，像某师傅一样优秀

多把基础打扎实点，以后还想做管理呢

规划是个啥玩意？

未来发展与规划-好与坏的平衡



未来发展与规划-骑驴找马，让伯乐自动送上门！

我驴在哪？怎么骑？

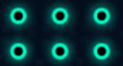
怎么让驴加速？

我的千里马在哪？

伯乐？来一斤....

FIT 2019

目录



白帽阶段转化引导

初级
- 对方喜欢玩啥，就让他玩啥
- 因为对方根本不知道有啥

中级
- 基于兴趣尝试一段时间的深度学习
- 因为对方不知道到底适不适合自己

高级
- 技术方向抉择，规划辅助，转型
- 因为对方经历的多就知道了

你给了建议，对方以为你在坑他。【有木有深有感触？】

白帽子转型职业工程师建议

建议一：人无完人，用全力，迎接你的职场

建议二：比你牛的人，一定汗水很多

建议三：谦虚谨慎，多低头学习做事情

建议四：要学会体现你的成果

建议五：急躁是解决不了问题的

建议六：成长是无限的，学习是首要的

建议七：别人的建议要去尝试验证和体会

建议八：扬长避短，查缺补漏

我的联系方式

邮件：admin@secbug.org

微信二维码

FREEBUF | FIT

THANKS