自学成才的黑客（安全研究员）是从哪学到那些知识的？

谢邀。

问题中“黑客”这词用的有点大，因为黑客代表的不仅仅是专业技术上的造诣，更包括了思想，思维，甚至是一种精神。

如今娱乐化严重的安全圈，“黑客”二字早已成为了面子工作者嘴里的谈资。

牢骚完了，下面根据上面说的分几方面说如何向着“黑客”努力。

有关技术：

现在获取信息的渠道越来越多，每天新增的技术文章早已超出了人能够处理的能力范围，如何发现精华，筛选，归类这些信息是很重要的工作。

本人较关注Web及移动安全，以下以此方向举例

1，Twitter： 首先定位一个你关注的方向，比如前端黑客，选一个关键词，不要选那种假大空的XXX Security，因为这种定位出来的信息一般都是扯淡类型的，选一个技术点：比如CSRF，DOM XSS，CSP Bypass，XSS Vector，去Twitter搜，看聊这些话题的人，一个一个翻，看他们的历史tweet，如果你感兴趣的比较多，那么关注之。然后一个一个过你关注的这个人 **所关注的人**，然后重复上述步骤。求精不求多，关注几个领域内的巨牛，他们的信息就足够你消化的了。

比如Web安全方面我关注了（本人@pnig0s）：

@k3170Makan（Android Security CookBook的作者，之前也是Web安全领域的牛，专业挖Google漏洞30年）

@irsdl（Web安全领域大牛，来自NCC Group）

@lcamtuf（Web安全，漏洞挖掘的神牛，来自Google安全团队）

@bulkneets（日本友人，前端安全牛，国外多个漏洞奖励计划榜上常客）

@kuza55（低调，总之牛就对了）

@kkotowicz（专注HTML5安全，大牛一枚，BlackHat等会议演讲者）

@0x6D6172696F（专注XSS）

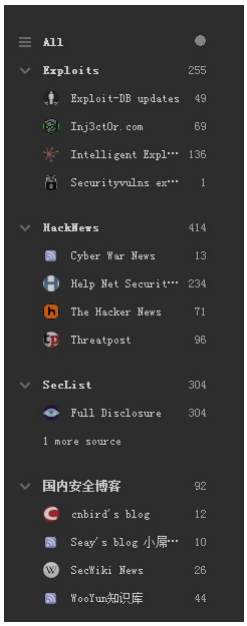
@shreeraj（前端神牛，多本Web安全书籍作者）

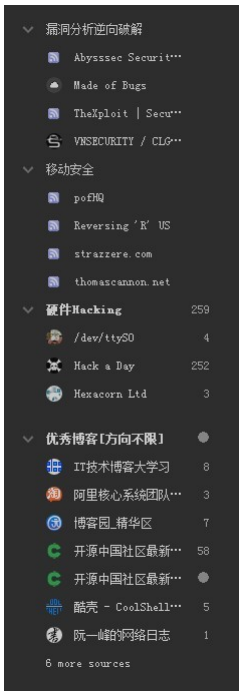
.....等等

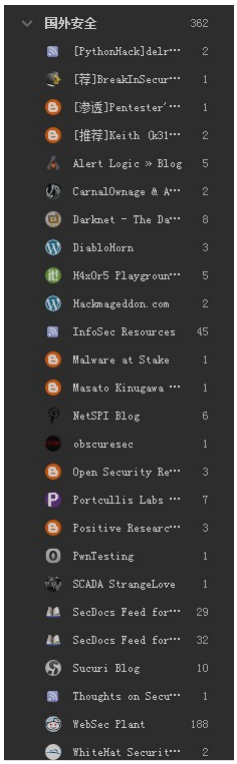
2，Blog：

不同领域的大牛都有自己的博客，所以，尽情的去挖坟吧。不要觉得人家文章过时了，没有意义。红遍大江南北的Struts代码执行漏洞也是被挖坟挖出来的，Android WebView任意命令执行漏洞也是11年就被研究出来了。所以，牛人的Blog很多几年前的东西现在看还是超前的，这不是盲从，谁挖谁知道。很多国内的牛都是读完了国外的Paper，总结一下，发散一下，然后发到国内来充大头的。

我用的订阅器是Feedly：







当然这些订阅我不会都看，每天会一目10行的过未读条目，如果标题第一印象我感兴趣，那么才会点进去看看，而且最关键的是一定要符合近期的研究方向。（订阅的内容本答案包括了一部分）

3，邮件列表及讨论组：

1） SecLists.Org Security Mailing List Archive

2） https:// groups.google.com/forum /#!forum/android-security-discuss

3）.....

4，安全文档Paper汇总：

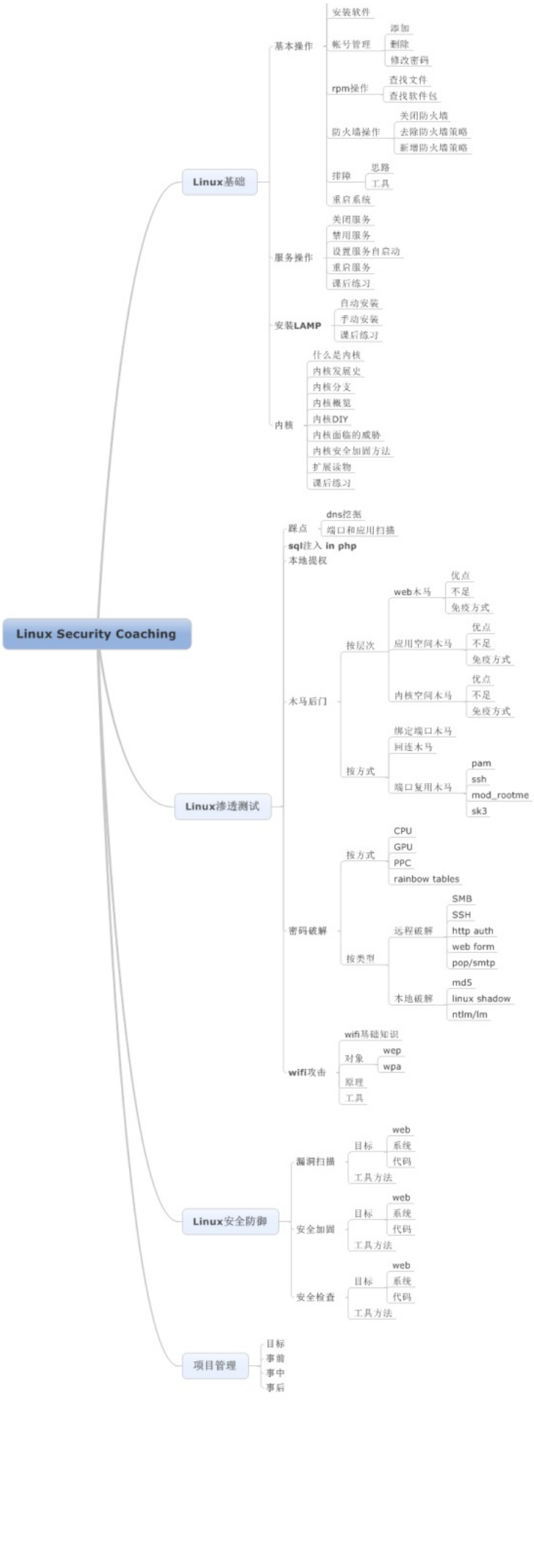
SecWiki-安全维基,汇集国内外优秀安全资讯、工具和网站

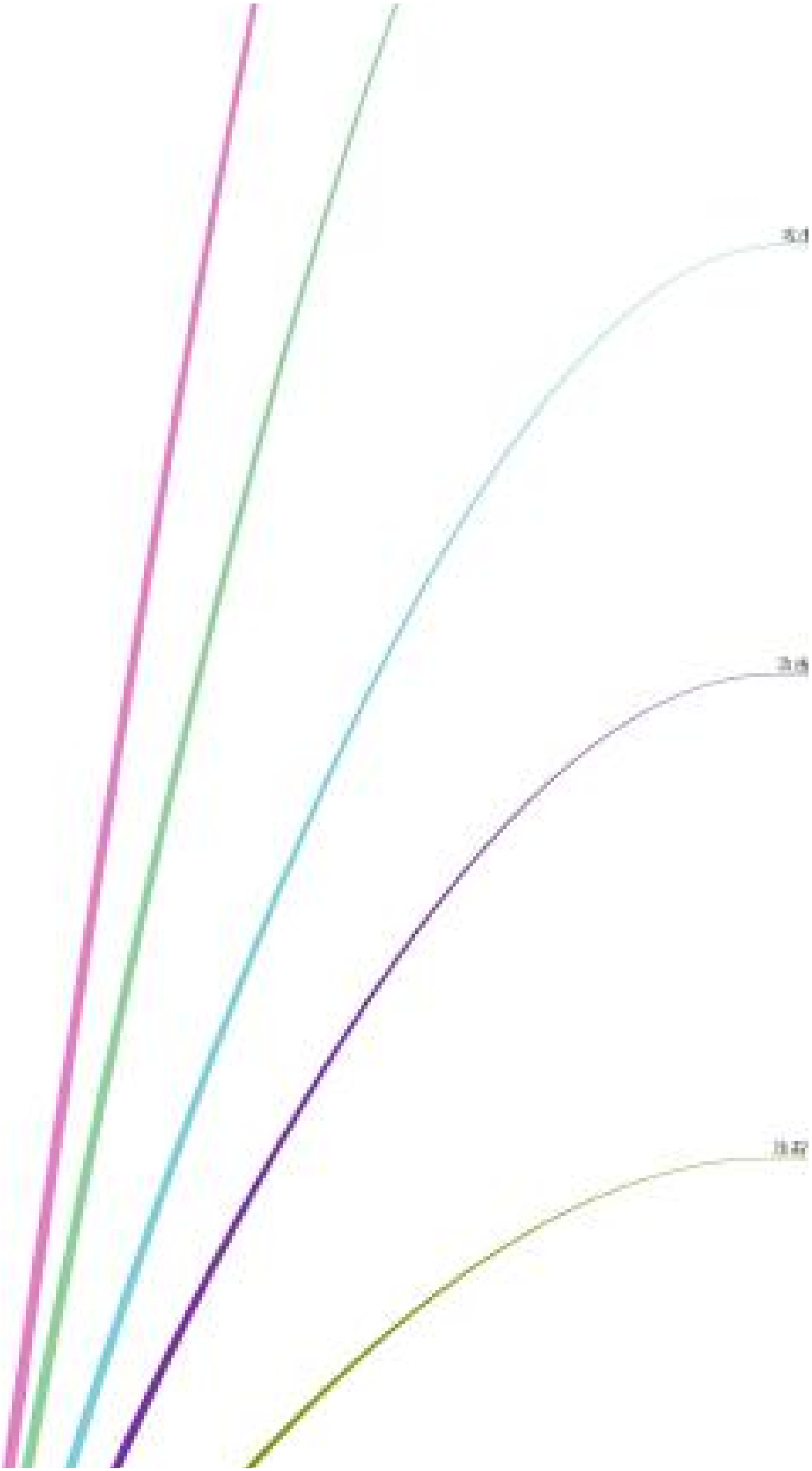
IT Security and Hacking knowledge base

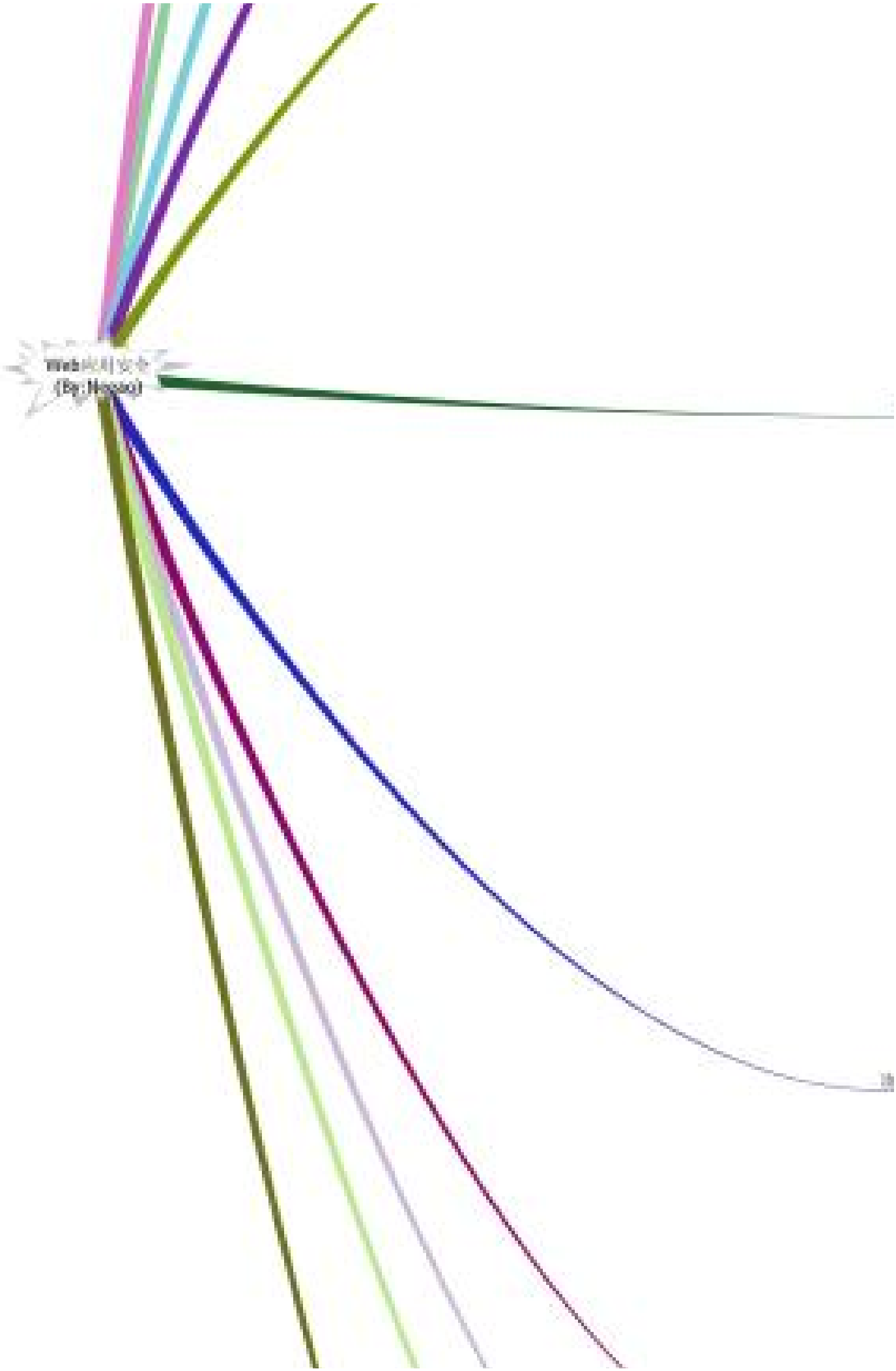
安全 文章 - FreeBuf.COM

WooYun知识库

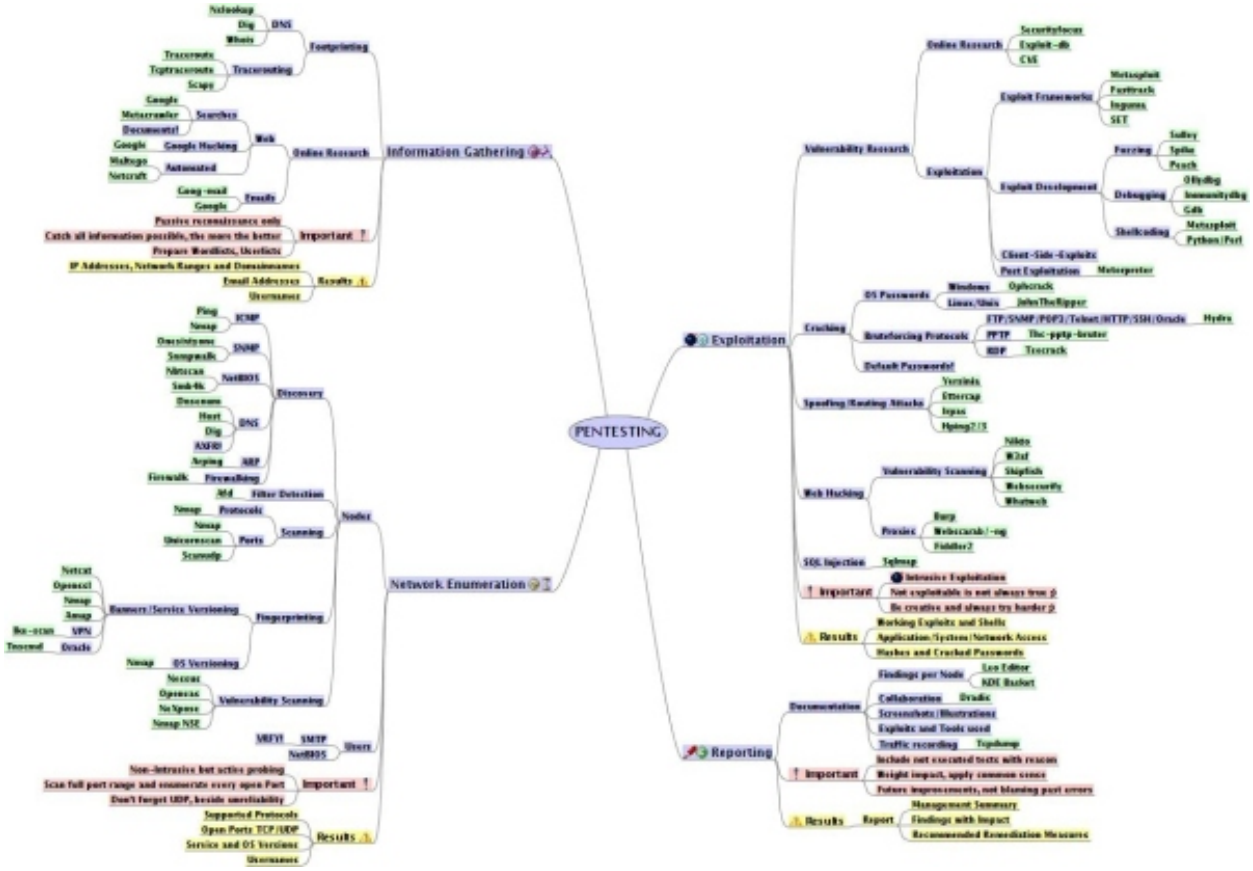
5，多找或制作思维导图（梳理思路）：

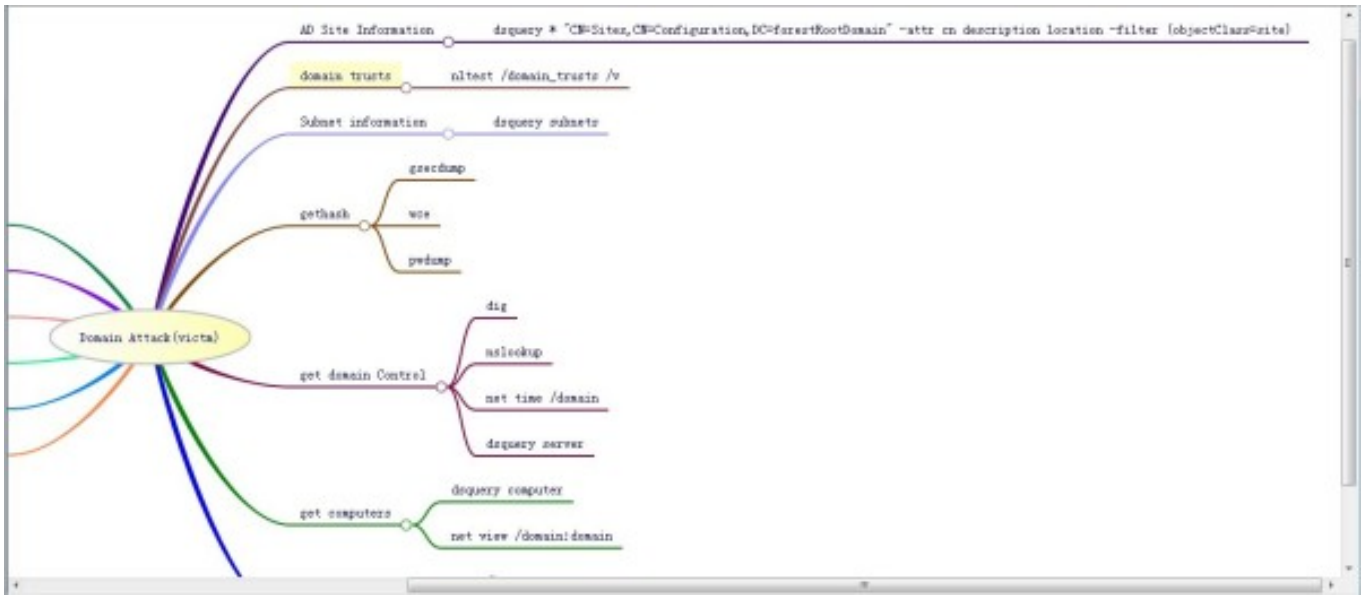

Linux Security Coaching
Linux基础
基本操作
安装软件
帐号管理
添加
删除
修改密码
rpm操作
查找文件
查找软件包
防火墙操作
关闭防火墙
去除防火墙策略
新增防火墙策略
排障
思路
工具
重启系统
服务操作
关闭服务
禁用服务
设置服务自启动
重启服务
课后练习
安装LAMP
自动安装
手动安装
课后练习
内核
什么是内核
内核发展史
内核分支
内核概览
内核DIY
内核面临的威胁
内核安全加固方法
扩展读物
课后练习
Linux渗透测试
踩点
dns挖掘
端口和应用扫描
sql注入 in php
本地提权
木马后门
按层次
web木马
优点
不足
免疫方式
应用空间木马
优点
不足
免疫方式
内核空间木马
优点
不足
免疫方式
按方式
绑定端口木马
回连木马
端口复用木马
pam
ssh
mod_rootme
sk3
密码破解
按方式
CPU
GPU
PPC
rainbow tables
按类型
远程破解
SMB
SSH
http auth
web form
pop/smtp
本地破解
md5
linux shadow
ntlm/lm
wifi攻击
wifi基础知识
对象
wep
wpa
原理
工具
Linux安全防御
漏洞扫描
目标
web
系统
代码
工具方法
安全加固
目标
web
系统
代码
工具方法
安全检查
目标
web
系统
代码
工具方法
项目管理
目标
事前
事中
事后






xss virus 1.0
依附平台
pc: windows/*nix操作系统
xss: web "os"
自启动
pc
随os启动而启动
启动目录
注册表Run方式
bootkit
xss
随web平台启动而启动
保证payload能够执行的各种方式
自我删除
完成任务后，自我删除
清理痕迹
传播性
pc worm
pc
挂马-->大批量挂马
感染移动盘，autorun
局域网arp等
xss worm
xss
感染服务端全局存储变量
感染这个web os里的共同特性：eg:共同好友
社工传播
不限于xss技术层面
与外域通信
木马性质：eg: xss trojan
从外域加载shellcode执行
实时执行某段js指令
盗取数据往外发送
牧鱼性质
pc
Q包
其它小窗广告
浏览器ads
xss
js dom动态生成钓鱼ui
登陆口
密码确认
各类伪信息暗示
xss robot
你好
我是xx网的机器人小艾
我们交个朋友
.....
未来
html5新特性
w3c cross-domain-access
xhr-XmlHttpRequst-ajax
xdr-XmlDomainRequest
分布式的
这也是云概念
消耗每个宿主浏览器资源
ddos
fuzzing
大数据量计算
...
潜伏隐蔽性
pc
驱动级保护
进程不可见
启动项不可见
注册表项不可见
服务项不可见
文件名混淆
爆发前说明显症状
类型
传统病毒
木马
downloaders下载者
蠕虫
xss
shellcode在第三方存储
src=http://romote.js
是普通的
eval(window.name)方式
shellcode保存在本地存储中
cookie
flash cookie
userData
localStorage
shellcode保存在后端数据库中
cod出现在其他页面内
使用ajax/dom将cod加载执行
网域
payload保护
ui上看不出任何痕迹
代码加密、混淆
思想：本质都一样
危害性
pc
破坏本地数据
盗取隐私信息
盗取各种账号密码
xss
破坏web平台数据--当前用户
盗取隐私信息
私有文章
私人资料
...
同样可以盗取各种账号密码
msn api
qq api
思想：web平台上同样有im的接口，盗号
原生态性质
win32 api强大的接口
pc
网络通信api
资源读写api
xss
email api
xml-rpc
内置的js框架，封装了很多nice的操作
思想：借用外力，保持代码短小而强大


PENTESTING
Information Gathering
Footprinting
Nslookup
Dig
DNS
Whois
Tracerouting
Traceroute
Tcptraceroute
Scapy
Online Research
Web
Google
Metasearcher
Searches
Documents!
Google Hacking
Google
Malkaga
Automated
Netcraft
Email
Gang-mail
Google
Results
Important
Passive reconnaissance only
Catch all information possible, the more the better
Prepare Wordlists, Unofficials
Results
IP Addresses, Network Ranges and Domainnames
Email Addresses
Usernames
Network Enumeration
Nodes
Discovery
ICMP
Ping
Nmap
SNMP
Onesixtyone
Snmpwalk
NetBIOS
Nbtscan
Smb4k
Dnsenum
DNS
Host
Dig
AXFR
ARP
Arping
Firewalking
FirewalkING
Scanning
Mtd
Filter Detection
Protocols
Nmap
Ports
Unicornscan
Scanudp
Fingerprinting
Banners/Service Versioning
Netcat
Openssl
Nmap
Amap
Vulnerability Scanning
Nessus
Openvas
Nexpose
Nmap NSE
OS Versioning
Nmap
Users
VRFY
SMTP
NetBIOS
Important
Non-Intrusive but active probing
Scan full port range and enumerate every open Port
Don't forget UDP, beside unreliability
Results
Supported Protocols
Open Ports TCP/UDP
Service and OS Versions
Usernames
Exploitation
Vulnerability Research
Online Research
SecurityFocus
Exploit-db
CVE
Exploitation
Exploit Frameworks
Metasploit
Fastrack
Inguana
SET
Exploit Development
Fuzzing
Sulley
Spike
Peach
Debugging
OllyDbg
Immunitydbg
Gdb
Shellcoding
Metasploit
Python/Perl
Client-Side-Exploits
Post Exploitation
Meterpreter
Cracking
OS Passwords
Windows
Ophcrack
Linux/Unix
JohnTheRipper
Bruteforcing Protocols
FTP/SNMP/POP3/Telnet/HTTP/SSH/Oracle
Hydra
PPTP
Thc-pptp-bruter
RDP
Tsecrack
Default Passwords!
Spoofing/Routing Attacks
Yersinia
Ettercap
Ipspa
Hping2/3
Web Hacking
Vulnerability Scanning
Nikto
W3af
Skipfish
Websecurify
Whatweb
Proxies
Burp
Webscarab/-ng
Fiddler2
SQL Injection
Sqlmap
Important
Intrusive Exploitation
Not exploitable is not always true :p
Be creative and always try harder :p
Results
Working Exploits and Shells
Application/System/Network Access
Hashes and Cracked Passwords
Reporting
Documentation
Findings per Node
Leo Editor
NDE Rocket
Collaboration
Drudic
Screenshots/Illustrations
Exploits and Tools used
Traffic recording
Tcpdump
Important
Include not executed tests with reason
Weight impact, apply common sense
Future improvements, not blaming past errors
Results
Report
Management Summary
Findings with Impact
Recommended Remediation Measures



二，安全资讯：
保持阅读安全资讯的习惯对于开阔视野，发散思维，提高创新的能力都是非常有帮助的，时常关心一下国内国外有哪些新的安全事件。通过安全资讯了解到一些你感兴趣的点，进而深入研究。要知道，资讯的传播速度和范围都要远远优于技术分析文章，所以先有技术资讯，后才有技术分析。如果一个不关注资讯信息的人，又怎么能知道在其所关注的领域有哪些创新的研究成果呢。
推荐：
作为FreeBuf的掌柜之一，我继续厚着脸皮推荐，因为我对内容有信心。
FreeBuf.COM关注黑客与极客 Cyber War News Help Net Security The Hacker News Threatpost | The first stop for security news
FreeBuf部分稿源翻译自以上站点及Twitter实时安全动态，所以你们懂得。

三，提升能力

1，想成为黑客，不能只关注在技术上，思维方式很重要，而且一定程度上决定了你牛的程度。技术其实就那些东西，牛和不牛之前相差的不是技术，是经验，而只有丰富的经验才会产生丰富的思路。所以我们不要总和技术点过意不去，一遍一遍的去重复一些我们已经掌握的技能。

以基本的数据库安全举个例子：

1. 第一天我学会了简单MySQL注入
2. 第二天我学会了MySQL注入的基于时间，基于布尔，基于报错的注入读库，表，列，数据。
3. 第三天我学会了通过MySQL读数据库路径，工作目录，服务端IP，链接端IP
4. 第四天我深入了解了MySQL4，和5数据库结构组成的差异，知道了数据库账密存哪儿，Hash是什么类型加密的，不同版本加密方式有什么不同，怎么破。
5. 第五天我学会了如何通过MySQL提权，在什么条件下提权，不同版本下提权方式有哪些不同。了解提权细节，如何写dll，加自定义函数。

主线大概是这样，然后，就是在一次次的实战去填充优化各种细节了。比如MSSQL，Oracle，无非是重复以上的步骤，MSSQL你还要知道各种存储过程哪些和安全有强依赖，哪些存储过程在什么权限下能够使用，默认哪个版本的哪个权限能操作哪些存储过程，这些都是细节，所以开始学习的过程中完成主线的任务即可，千万不要陷入细节中，否则容易走火入魔，万劫不复。比如Oracle相关的安全问题，研究过的人大概都会说“What a mess！”

2，多实践：
比如研究个DOM XSS，看了很多paper还觉得太乱，没法贯通，怎么办？写个DOM XSS检测模块出来，在这个过程中会逼着你自己去了解透彻，一步步实践，一点点清晰。最后完成的时候，一切都通透了。读的再多也是别人的知识，实践到手上才能转化为自己的营养。一遍遍说，但只有做下来的人才知道它的意义。

3，多总结：
写Blog也好，写Note也好，或者总结成正式的paper也好。要不停的做笔记，总结，总结是一个提炼，回炉重造的过程，读进脑子里的是别人的语言，自己总结出来的是自己的语言，更便于记忆和理解。一遍遍说，但只有做下来的人才知道它的意义。

写到最后我感觉已经跑题了，总之知识的来源真的不需要太多，也不用过分关心。不同的时代知识的来源各有优劣，但却总能造就出牛人，关键就是能够踏实下来做，你不停的做下去，知识也会不停的涌现出来，不用刻意的去找。

引用heige的一句话“整就牛。”

再引用某人的一句话“能安静下来做事的人会成为大牛，能随时随地安静下来做事的人会成为大神。”

【2,31UPDATE】

很多人问我要RSS订阅的列表，我先给份儿公开的 BookmarksList

不经过自己辛勤整理出来的东西自己也不会去认真看的，上面那份非常完整，我收藏了但基本不会看，因为我没怎么付出。反而经常看我自己整理的那份残缺的版本，因为我更了解，更符合我的关注点。所以各位还是自行整理吧，整理的过程也是在学习：）

安全行业优质的微信公众号推荐？

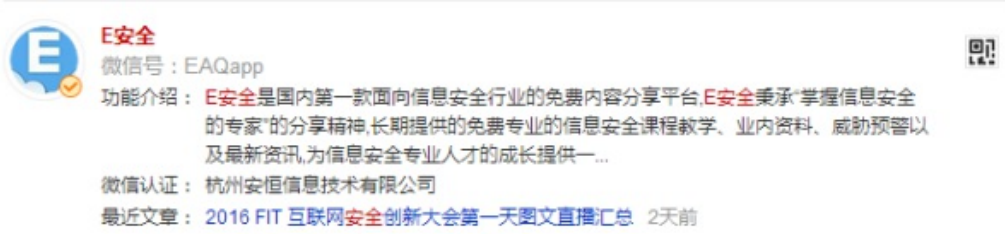
微信公众号的推荐，在知乎上也是有过一些提问。但是针对安全圈，好像还真没有一个系统的问答。

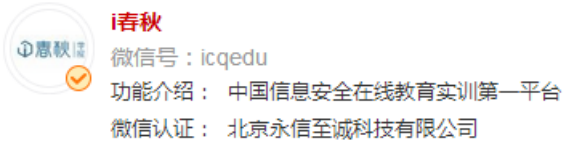
作为一个刚刚加入安全圈的运营妹子，我的手机已经关注了很多很多微信公众号了，有个人的，有企业的，同样也有各大SRC，下面给大家分享一下。

一、各大SRC

各大SRC，其实主要是关注，BAT，小米，360，滴滴，京东，携程，唯品会，这样的是最官方的，然后活动送票，送礼品，最新众测项目都会从这里发出来~

二、各大安全媒体

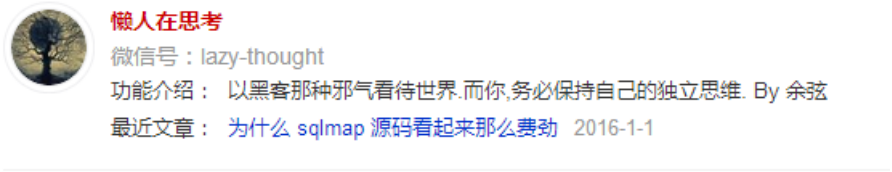


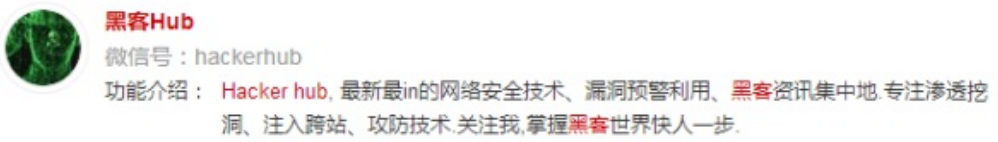


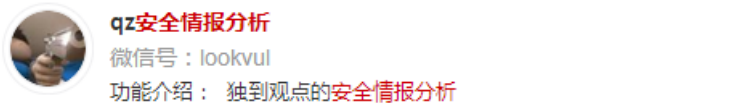
这些，小编一般会经常看安全，freebuf，安全优佳，还有E安全

继续补充....

三、一些大牛自己运营的微信号，也很值得关注，有技术有运营，有评论







301在路上

微信号：a301zls

功能介绍： 分享最新的互联网安全动态、分享最有意思的安全资讯内容,关注最真实的白帽子黑客,做最简单的安全自媒体.301一直在路上.301个人公众号与所在单位乌云网无关.如有问题可留言(必回复)

四、当然也有一些非常用心的小伙伴自己运营的微信号，也是很不错的

酷安全

微信号：koosec

功能介绍： 分享我知道的,收藏你需要的.

五、众测平台也是不能少的
乌云，Sobug，威客安全（原威客众测），ASRC，TSRC，BSRC，VSRC，DSRC等等

今天先整理这些，再慢慢补充~

作为一个刚加入安全圈的妹子，需要学习的太多了~ 感兴趣的小伙伴可以私信我哦~

共进步！

原创分享：推荐几本安全方面的好书

今天给大家推荐几本安全方面的好书，希望对大家的提升有所帮助

还有一本无线攻防，那个四本书，是我们打算公司内部 培训 用的。

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

下面那些书，来源杨卿，朋友圈，

杨卿，出了一本无线电攻防，我还没买呢，打算定5本，听说不错。

想学知识吧，还是得从书本里看，有一些基础的东西，还是需要一点点去实践，去练习的。网上全是碎片化的信息，不能补全自己的知识点。

风络安全几个技术级别：

网络工程师 >> 系统工程师 >> 软件工程师 >> 安全

想从事安全这个行业，还需要了解 网络工程师的知识，系统工程师的知识 ，软件工程师的知识，最后你才能修练成网络安全工程师，不是怎么简单的一个过程 ，是一个修练的过程。

为什么加入这个行业?

炫酷、成绩差、捷径、挑战、黑客精神
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

中国网络安全发展趋势：

信息安全时代 >> 网络安全时代 >> 互联网安全时代 >> 移动安全时代 >> 智能安全时代

作为网络安全技术人员你必须准备：

耐得信寂寞;

累成狗;

黑白颠倒;

不受诱惑;

赚钱不多(行业估值不高)

遵从黑客精神：

拥有一颗探索的心;

拥有一颗低调的心;

不包装和显摆;

在技术领域里得到自我认同;

不去获得非法利益

祝大家早日成材～～踩着我们的肩膀攀登高峰!

来源：华盟网，作者：怪狗，

未得授权禁止转载