

零基础/进阶系统化白帽黑客学习指南 | 12月份

原创 HACK学习 HACK学习呀

2019-12-07原文

0X00 介绍

有些人学习完全可以自学，但有些人总是需要别人的帮助，HACK学习的白帽培训班正式上线，给予那些想学习又没有自学能力或者说有能力但是感觉学习很吃力的同学一个好的入门途径！

现今网络上黑阔遍地走，小学生多如狗！贴吧，论坛，部落，QQ群，随处可见，打着收徒名义招摇撞骗的，刷钻的，盗号的，改成绩的，我就不一一列举了，与其四处求学被骗不如来我们这里报名！

报名前，我希望大家阅读以下几篇文章，以免学习后滥用技术做犯法活动

中华人民共和国网络安全法

http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm

黑产牛，万一你被抓了呢？所以你需要知道这些！

<https://www.t00ls.net/articles-53566.html>

搞黑产，算算你能判多少年？

<https://www.t00ls.net/articles-35804.html>

互联网帐号恶意注册和养号黑色产业的刑法思考

<https://www.t00ls.net/articles-53053.html>

提供侵入、非法控制计算机信息系统程序、工具罪

<https://www.t00ls.net/articles-52907.html>

侵入后的动作法律解析

<https://www.t00ls.net/articles-51183.html>

网络传销的法律后果

<https://www.t00ls.net/articles-38183.html>

侵犯公民个人信息相关

<https://www.t00ls.net/articles-52907.html>

侵入后的动作法律解析

<https://www.t00ls.net/articles-51183.html>

网络安全法之网络隐私权

<https://www.t00ls.net/articles-40280.html>

超出授权范围侵入计算机信息系统

<https://www.t00ls.net/articles-47493.html>

看看传播“私密小视频”的后果

<https://www.t00ls.net/articles-35861.html>

破坏计算机信息系统罪和非法入侵计算机信息系统区别

<https://www.t00ls.net/articles-46171.html>

以上内容来自T00ls普法贴，希望你认真去读一读，以上帖子均可访问，无须登录

技术是一把双刃剑，可以做好事，当然也可能将你自己送进监狱

总而言之，遵纪守法、NO ZUO NO DIE

学好技术，然后找一份好工作，为社会做贡献，学好网络安全为人民

0X01 学习模式

学习模式：

加密视频+专属答疑+引导安排课程学习计划+实战指导+学习笔记+实战案例分享+找工作前的模拟面试+安全行业职业生涯规划建议

学习时间：

学习时间可以自己安排，不受任何其他人的限制，按照我们的阶段安排走就行

模式优势：

半自学的模式有利于培养自己的实操能力和主动思考方式以及优秀的自主解决问题的能力

如何答疑：

当然我们会给你必要的答疑和帮助以及QQ远程协助，包括内部社区

如何监督：

内部社区监督学习，练习以及非实时的问题解答等

0X02 内部社区

内部社区：bbs.tesla-space.com【未登录用户是无法查看相关内容的】

后台首页

站点统计信息

主题数：2152

附件总数：4729

帖子数：4727

在线人数：8

HACK学习呀

4000+ 学 习 笔 记 以 及 学 习 案 例 & 答 疑 解 惑 贴

4000+附件，包括pdf资料，脱密实战案例，渗透技巧思路等

HACK

[首页](#)
[代码审计](#)
[安全工具](#)
[渗透测试](#)
[学习笔记](#)
[无线安全](#)
[硬件安全](#)
[提问&答疑](#)
[内部学习资料](#)
[漏洞挖掘](#)

消息

退出

每日一句: A man can fail many times, but he isn't a failure until he begins to blame somebody else. 一个人可以失败很多次, 但是只要他没有开始责怪旁人, 他还不是一个失败者。

HACK学习

最新 精华

HACK学习入园必读公告

HACK学习 2018-6-17 hhd 7小时前

336 306

圈子奖励计划开启

HACK学习 2018-6-30 naodafeng 6天前

69 116

【更新预告】本周末将更新漏洞挖掘案例以及更多渗透测试文章

HACK学习 2018-8-30 xinyu 17天前

49 94

【精华】收集的网络安全学习网址

HACK学习 2018-10-28 DA617 5天前

51 59

【零基础必看贴】从小白到“大神”的成神之路——搜索引擎该怎么用?

HACK学习 2018-10-31 xiaobai 2天前

65 73

发新帖

签到

连续签到1天

HACK学习内部圈子

HACK学习内部圈, 仅供HACK学习内部学员使用交流, 暂不对外开放, 如需加入圈子, 请提交原创漏洞稿子或者挖洞心得, 以及优质的技术文章, 经审核通过后, 即可注册邀请码

关键词

搜索

经典名句

人生不是一种享乐, 而是一桩十分沉重的工作。 - 列夫 托尔斯泰

友情链接

[HACK学习官网](#)
[HACK学习内部圈子](#)
[威胁魔方-知识体系](#)
[【安全社区】先知社区](#)
[【安全社区】FreeBuf](#)
[【优质博客】信安之路](#)

内部XSS平台:

OA SYSTEM

Index

个人设置

IP-URL黑名单设置

邀请码

超管后台

退出登陆

我的项目

创建

1 - [项目ID: 7]

我的模块

创建

公共模块

[~Jsonp社工模块~](#)
[post指定页面源码读取](#)
[获取内网ip](#)
[JetBrains远程命令执行](#)
[JetBrains ide任意文件读取](#)
[键盘记录](#)

项目内容

配置 查看代码

项目名称: 1

Domain: 全部 此处可选择需要查看的域名

| | 时间 | 接收的内容 | Request Headers | 操作 |
|---------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| +全部 | | | | |
| -折叠 | 2019-11-04 22:54:25 | <ul style="list-style-type: none"> location : http://1/vulnerabilities/xss_s/ toplocation : http://41/vulnerabilities/xss_s/ cookie : PHPSESSID=ths4j8olt5c2fjun94smorfnc7; security=low opener : | <ul style="list-style-type: none"> HTTP_REFERER : http://21/vulnerabilities/xss_s/ HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36 REMOTE_ADDR : 113 REMOTE_PORT : 44764 IP-ADDR : | 删除 |

选中项操作:

删除

1 共1页

公共模块

-Jsonp社工模块-

post指定页面源码读取

获取内网ip

JetBrains远程命令执行

JetBrains ide任意文件读取

键盘记录

自动获取内网ip打内网redis

xss+csrf+redis自动化入侵内网

CSRF操作Redis写文件

获取页面源码

获取浏览器记住的明文密码

HTML5截屏

基础认证钓鱼

xss.js

AJAX POST/GET操作

apache httponly bypass

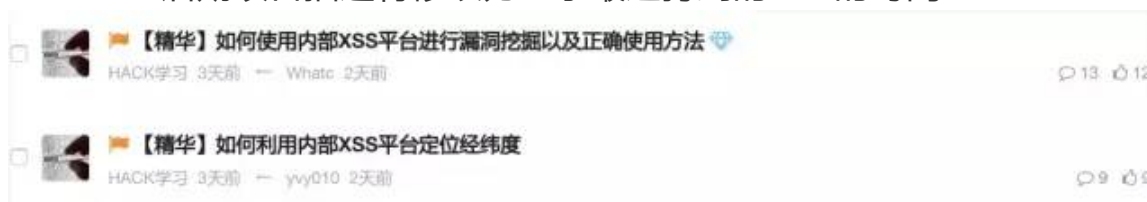
默认模块

HACK学习网

XSS平台修改为可以打到IP和端口，对IP落地有帮助



后期项目描述将修改为显示最近打到的XSS的时间



内部社区价值:

内部圈子是为了提升和监督学员内部间交流分享，共同学习进步的圈子

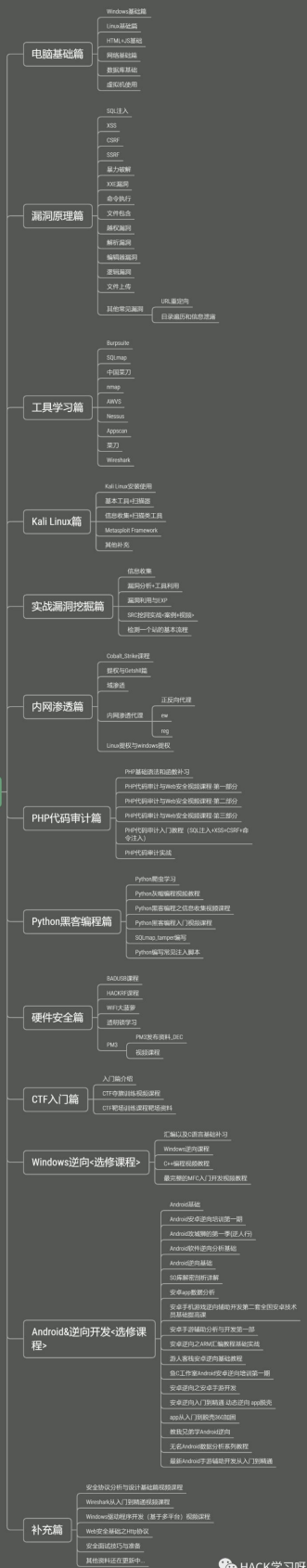
内部社区会经常更新漏洞挖掘实战案例，让大家学习姿势，以及新增提问区，每个学员有问题可以随时在社区发帖提问

报名后会给内部社区邀请码以及内部XSS平台的邀请码

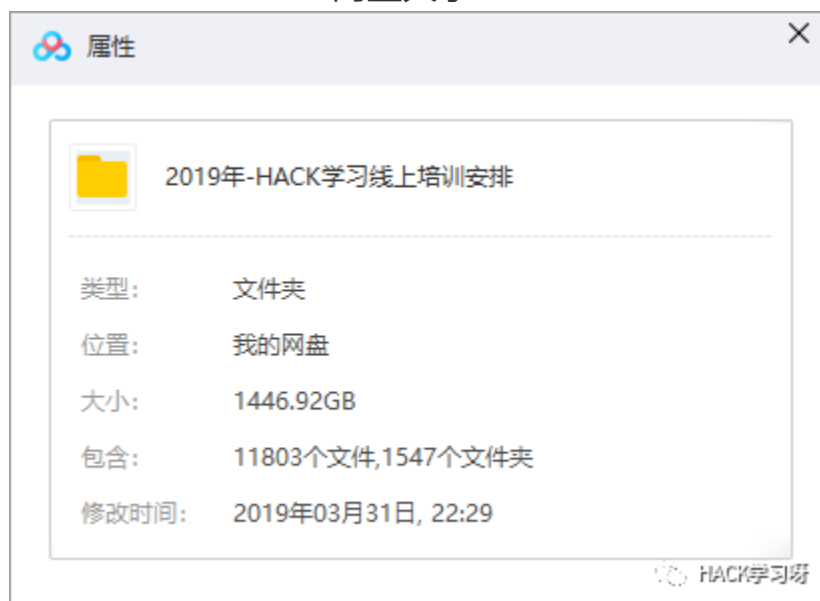
<更多社工定位模块敬请期待>

0X03 课程安排

HACK学习课程框架



详细目录，请联系文末报名微信获取
网盘大小：



| <div> <div> <div></div> <div></div> <div></div> <div></div> </div> <div>我的网盘 > 2019年-HACK学习线上培训安排 ></div> </div> | | | |
|------------------------------------------------------------------------------------------------------------------------|------------------|----|--------|
| 文件名 | 修改时间 | 大小 | |
| <input type="checkbox"/> 2019渗透测试-Web安 | 2019-04-04 14:10 | - | |
| <input type="checkbox"/> 补充资料篇 | 2019-04-04 09:44 | - | |
| <input type="checkbox"/> 第八阶段-硬件安全课程 | 2019-04-04 09:38 | - | |
| <input type="checkbox"/> 第二阶段-Web安全篇 | 2019-04-04 20:05 | - | |
| <input type="checkbox"/> 第九阶段-CTF课程 | 2019-04-04 09:41 | - | |
| <input type="checkbox"/> 第六阶段-Python黑客编程 | 2019-04-04 09:41 | - | |
| <input type="checkbox"/> 第七阶段-PHP代码审计 | 2019-04-04 09:41 | - | |
| <input type="checkbox"/> 第三阶段-Kali Linux | 2019-04-04 09:40 | - | |
| <input type="checkbox"/> 第十二阶段-更多更新 | 2019-04-04 13:53 | - | |
| <input type="checkbox"/> 第十阶段-漏洞挖掘技巧 | 2019-04-04 13:03 | - | |
| <input type="checkbox"/> 第十一阶段 | 2019-05-13 14:57 | - | |
| <input type="checkbox"/> 第四阶段-实战渗透篇 | 2019-04-04 09:41 | - | 🔊 ⬇️ 📄 |
| <input type="checkbox"/> 第五阶段-内网渗透篇 | 2019-04-04 09:40 | - | |
| <input type="checkbox"/> 第一阶段-基础篇 | 2019-04-04 09:27 | - | |
| <input type="checkbox"/> 附赠资料 | 2019-03-31 22:32 | - | |
| <input type="checkbox"/> 加密视频专用播放器 | 2019-10-09 12:54 | - | |
| <input type="checkbox"/> 以及漏洞挖掘课程-2018年录制 | 2019-07-20 18:01 | - | |
| <input type="checkbox"/> 选修部分-Windows逆向 | 2019-04-04 09:39 | - | |
| <input type="checkbox"/> 选修部分-安卓开发与安卓逆向 | 2019-04-04 09:41 | - | |
| <input type="checkbox"/> 学习笔记 | 2019-03-31 23:55 | - | |

资料包含：

高清晰度课程视频+必备虚拟机镜像环境+补充的安全书籍以及渗透文章+独家物理渗透课程[badusb+透明锁+Hackrf入门+PM3入门]

害怕资料太多，不知道该怎么学，不用担心，看文章后面，我们会安排每阶段的重点内容和学习计划

每个月都会更新增加内容：

2019年11月份更新内容

C#开发基础学习<方便后渗透学习免杀和shellcode编写混淆>

内网渗透课程

2019年10月份更新内容

Kali Nethunter[把手机打造成渗透系统]

Csploit玩法详解

2019年9月份更新内容

PHP代码审计[1-10部分]-漏洞挖掘【18-19年录制】

ps：内容比较丰富，详细目录联系报名微信获取

SQL注入的绕过/防御【19年录制】

2019年8月份更新内容

代码审计专题【19年录制】

文件上传姿势绕过【19年录制】

2019年7月份更新内容<免杀学习/SRC漏洞挖掘/TP框架代码审计>

:

Web漏洞SRC漏洞挖掘课程【19年录制】

价值8K的渗透测试课程【18年录制】

价值2K的远控编写与免杀课程【19年录制】

ThinkPHP代码审计【18年】

2019年6月份更新内容<漏洞利用学习>：

WinRAR远程代码执行漏洞结合演示

PHPmyadmin4.8.1文件包含漏洞利用getshell

Structs2远程代码执行漏洞测试

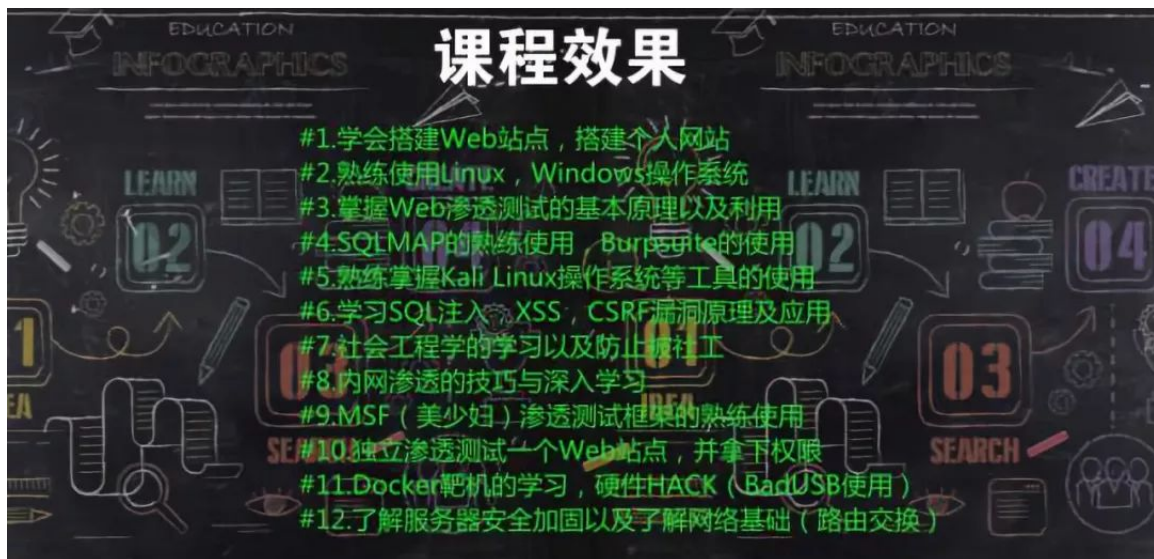
如何利用HFS漏洞获取权限

PHPMyadmin2.X反序列化漏洞

Imagetrack命令执行漏洞CVE2016-3714

Nginx文件上传解析漏洞复现
IIS短文件漏洞利用讲解
Tomcat任意写文件漏洞CVE201712615
apacheisapi漏洞利用
Nginx文件名逻辑漏洞CVE20134547
如何利用IIS_PUT漏洞获取权限
Drupal远程代码执行CVE20187600
Discuz7.x及6.x代码执行SQL注入利用
实例某cms注入漏洞挖掘
MYSQL突破Secure模式实现写shell
Discuz漏洞利用脚本编写
Thinkphp5.X代码执行漏洞利用
HFS漏洞利用脚本编写
利用Windows特性高效猜测目录

课程效果



13.掌握安卓逆向破解，安卓逆向破解小游戏，静态调试，动态调试，Smail，So文件逆向

14.掌握开锁技巧，透明锁练功锁开锁学习，学习物理黑客第一步

15. 熟悉 Kali Linux 操作系统，熟练掌握 Kali Linux 的常用工具和 Github 上开源工具的学习以及使用
16. 掌握局域网安全相关知识点，ARP 攻击以及中间人攻击等
17. CTF 入门学习，带你走进 CTF 赛事的大门，为以后参加 CTF 赛事，打下必备的基础
18. 独立渗透测试指定站点的能力【有授权的前提下，拒绝任何黑灰产】
19. PHP 代码审计以及 Python 黑客编程的学习，包括 Python 网络爬虫，编写 SQLMAP tamper，编写信息收集的脚本，暴力破解工具等
20. 独立挖掘漏洞的能力，在各大 SRC 平台提交漏洞以及独立挖掘众测的漏洞，赚取赏金等
21. 课程还在不断完善中，一次报名，终身学习！！

0X04 疑惑解答

常见报名学习前疑问与解答，可能有您的疑惑与解答哦

1、零基础可以参加培训学习吗？

答：HACK 学习的白帽黑客渗透测试培训课程，专门为零基础和有一点编程经验的朋友定制的，一张白纸更适合学习，有基础的人反而有些飘，通常零基础学的会更好，高手都是从零基础开始的。

2、需要多长时间才能学会？

答：参加培训之后，只要按照我们的课程学习，三 - 四个月就可以入门，一般6个月左右，可以系统全面熟练进行渗透测试，写渗透测试报告，并且自己动手编写小脚本程序（Python），解决实际问题。

3、培训的形式？

答：当期报名同学一起学习，高清视频课程+学员私密QQ群+课程PPT外加课外习题，以及同学的习题案例解答。

4、英文和数学不好，能否参加培训？

答：完全能参加，一点问题都没有。我本人也是英文和数学基础一直不太好，编程需要记住的单词就那么固定的几个，每天接触，很快就熟记于心了。

5、培训指导时间有多久？

答：一直有指导，学业结束后，会有长期的售后支持，以及内部社区讨论！

6. 学生、上班族时间不固定怎么？

答：HACK学习的培训课程采用视频录制为主特点+直播答疑+QQ远程协助，时间比较紧的同学，老师会紧跟每位同学的学习进度，视频内容可以随时下载，进行观看，不耽误工作和学习时间。

7.关于电脑配置

答：推荐使用i3或i5处理器【其实G4560我也用过，也没毛病/滑稽】，同水平的AMD处理器也可以，运行内存推荐8g以上，因为需要使用虚拟机搭建实验和练习环境，所以电脑中等配置左右就可以了。

8.不懂英语，不懂编程，数学不好可以学吗？

课程会讲到编程的，这点不用担心，不懂英语没关系，不用背单词，用着用着就记得了

9.学历不高能学吗，年龄大了能学吗？

与学历年龄无关，有兴趣才是最重要的，会用电脑就行。任何技术，任何行业，任何事情，兴趣才是第一位。

10.是在线授课吗，会有直播吗？

不是在线授课，后期会有直播解答以及普及一些自己正在研究的新东西

11.学习是否有时间限制？

没时间日期限制，几年后都可以学。几年前的老学员提问，我今天都在耐心的解答他的学习问题。

12.你能保证我学会吗？

我不能保证，我只能保证有问必答。只有骗子才能保证你能学会，因为学习是你自己的事情。

13.一般需要多久学会？

如果是零基础什么都不懂，大概需要4-5个月可以独立渗透和搭建各种服务和漏洞测试以及挖洞。具体还要看你的学习情况。

14.学多久能精通？

谁敢说自已精通？任何行业都是学无止境！活到老学到老！不断学习才能使自己更强！

15.是否以后还会找理由变相收钱？

不会。我这里没有太多的承诺，但是我的承诺基本上都可以兑现。

16.能有什么工作岗位？

Web安全工程师，渗透测试工程师，安全服务工程师，等保测评工程师与网安相关的行业

17.你能保证我找到工作吗？

我不能，这个问题和上面那个“你能保证我学会吗？”是一个概念。骗子才能保证你。自己的事情自己要付出努力才有希望。

18.那你能保证什么？

我能保证我不跑路，只要你想联系我，我不敢承诺下一秒就回复你，因为我不是机器人，但是最晚不会超过12小时，肯定回话。我还能保证解答你的学习问题，让你节省大量时间与学习烦恼。助成功。

0X05 学员案例

学员一，入职深信服

当然绝大多数功劳还是自己努力

愿意去学习去折腾练习

22:32

4G+ 90%

< 99+



[Redacted Name]



OK



我试试



好了



谢谢老大

星期三 13:04



老大，很感谢您

发送

HACK学习呀



深信服录用通知(实习生) -



录用通知书 (实习生)

您好! 首先, 恭喜您通过了所有的面试, 欢迎加入深信服大家庭!

录用信息如下:

- 1、 报到时间: 2019 年 7 月 12 日
- 2、 报到地点: 北京市西城区白纸坊东街 2 号经济日报社 A 座综合楼四层
- 3、 职位: 安全服务工程师 (实习)
- 4、 工作地点: 北京
- 5、 实习工资

相关薪资待遇信息请严格予以保密, 本录用通知书有效期为一个月, 自发出之日起生效。

深信服科技股份有限公司

2019 年 7 月 8 日

学员二，渗透岗，年薪19万

当然他的学历也很好，本科毕业，工作中的进步应该更快
基础底子不错，实际工作中能学到

19:28

HD 55%



iPhone 6s (玫瑰金)在线 - 5G

SVIP6



在不在

嗯

19:27

【深信服科技】亲爱的同学，
好！再次恭喜您通过我们所
...面试环节，成功收到我司
2020届校园招聘OFFER。我们
诚挚邀请您参加深信服2020届
校园招聘... OFFER沟通
会，届时，您将进一步了解我
司的具体情况以及签约的相关
事项。本次OFFER沟通会具体
安排如下：
【时间】9月25日下午14:00
【地点】...
【注意事项】请携带纸质版三
方协议参加沟通会

感谢您

谢谢你，老大

可以的

学了这么久

真的谢谢您

HACK学习呀



年底和这个学员约个饭先

学员三，漏洞挖掘，赚回学费

15:00

4G+ 62%

< 回炉

...



老大那个我今天挖到一个，用户遍历，密码爆破，信息泄露 我是做一次提交吗



标题是不是某某某网站存在用户遍历，密码爆破，信息泄露



😂😂😂

是的

可以的



okok



进群学习三个月已经回本了 😄😄
😄



还赚足了 😂😂

14:56

可以可以



15:01

4G+ 61%

< 回炉再

可以可以

非常 nice 啊

那我

哈哈哈哈哈可以的



5.14 进的群

哈哈哈哈哈

可以写下挖洞心得放社区里面了

哈哈

okok





我的资料

设置



2019年05月14日加入该群



群聊等级已达LV8



最近发言于刚刚



VIP 10枚



还未开通任何服务特权



我的空间



我的状态



拍摄我的状态

精选照片



编辑资料












发消息

HACK学习呀

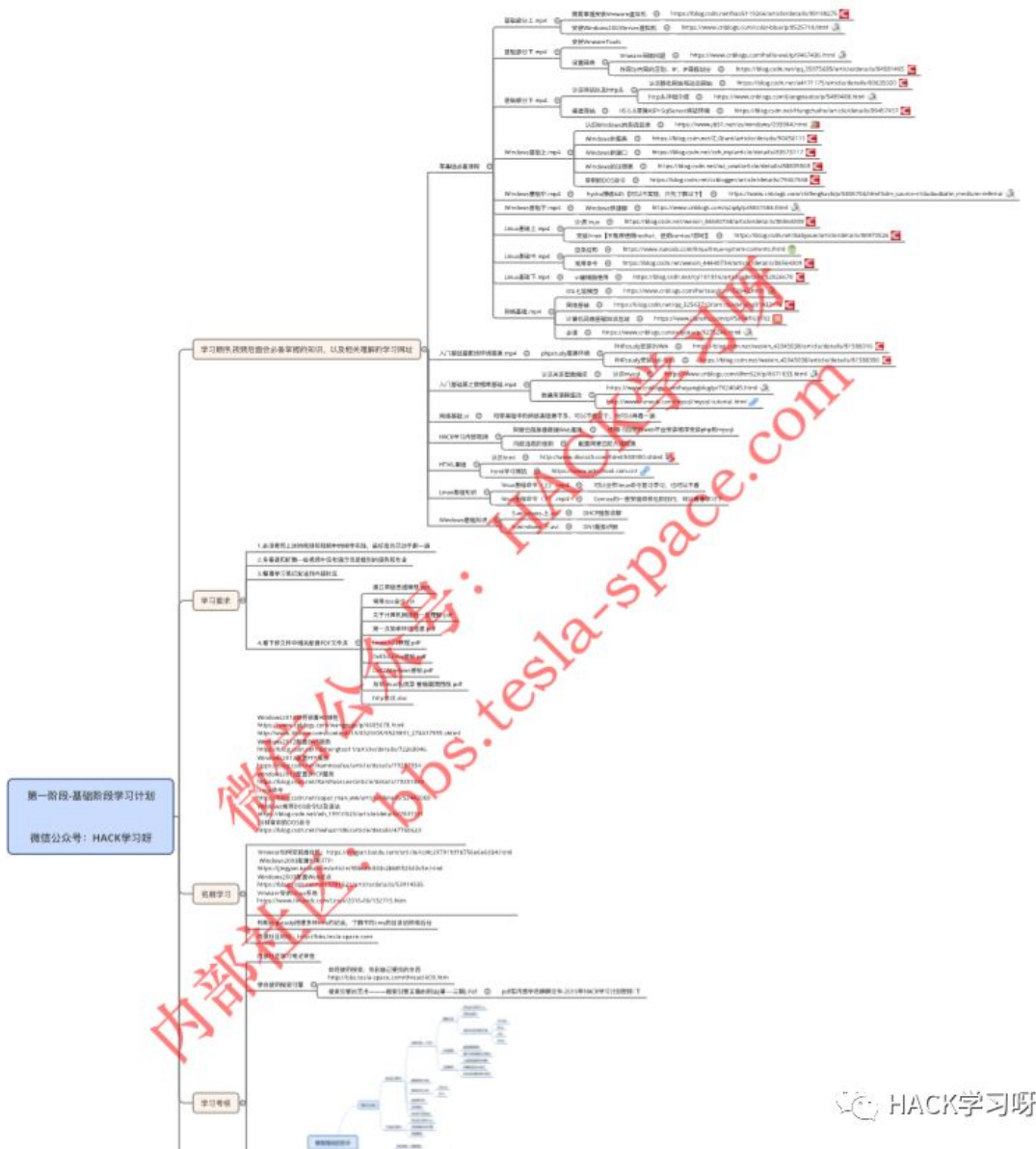
更多学员案例就不一一介绍了

0X06 课程学习计划安排

内部群

| | | | | | |
|--------------------------------------------------------------------------------------------------------|------------------|---|---|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  SRC漏洞挖掘以及渗透测试实战案例 | 2019-10-31 19:09 | - | - | - |  |
|  第二阶段-学习计划安排 | 2019-10-20 15:11 | - | - | - |  |
|  2019HACK学习计划安排【入群必看】 | 2019-10-20 15:07 | - | - | - |  |
|  安全书籍 | 2019-10-20 15:03 | - | - | - |  |
|  第一阶段-基础阶段学习 | 2019-10-14 22:14 | - | - |  HACK学习呀 |  |

第一阶段安排



高清版请联系报名微信

微信上传的图片可能不是很清晰，实际中PDF文档架构图片非常清晰
但是我们会安排的很细致，包括每一阶段要掌握的内容
以及重点和拓展了解的文章

0X07 报名费用以及报名流程

报名费用：600元【无任何后续收费,支持花呗支付】

报名优惠：分享到本图文到朋友圈或者QQ空间，即可减免50元，仅550元

报名流程

1.添加报名微信



微信号：X175144340

2.加报名微信后，付款转账【支持支付宝&微信转账】

3.邀请加入QQ群以及添加网盘以及资料发放

学员群不会解散的，这点放心

正式学习日期：报名即学，视频课程资料已下发到学员群文件和网盘分享

如果你想成为一名白帽黑客，想系统的学习入门

我们会是你的一个选择，当然，你也可以选择其他的学习地方
也可以根据我们的课程框架，选择自学，也很好，白嫖你又不吃亏
希望是可以帮到大家的，学习路上，多踩坑是好事，但是会耗费时间
看你自己怎么取舍了

或许你觉得这么多内容，怎么才600元，会不会是骗子

我们想说：我们也是从学生和初学者过来的，我们知道这其中有多少坑，有多少不可言喻的麻烦事，我们只想给予那些想系统化学习的小伙伴帮助

网上QQ群咸鱼一大堆地方1000收徒，2000收徒的比比皆是
课程内容你也可以对比下，我们丝毫不虚

一个简单，温馨，可靠的学习氛围和资料社区，以及前人的碎碎语，或许让你少走一些弯路而已

PS：我们不接受任何违法犯罪的学员报名学习，如果你有歪心思，请不要联系我们，我们只想传播更多正义，而不是黑灰产从业者，我们不提供任何犯罪技术教学！！



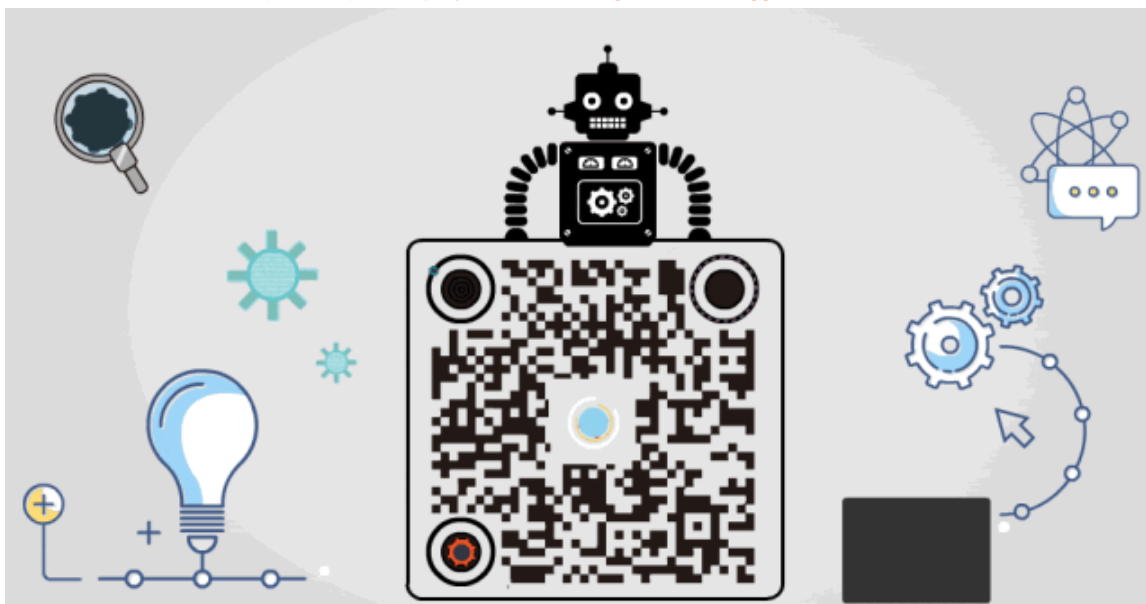
期待你的加入

一入安全深似海，从此游戏是路人

团队成员都是就职于国内某安全公司的安全工程师/渗透测试工程师

非黑灰产从业人员，希望大家都可以利用自己的所学，养活自己

为社会贡献更多安全力量，打击网络犯罪



精选留言

用户设置不下载评论