

点亮星河

成长型信安团队培育的几点体会

山东警察学院 张璇

0con 2016.4

关于我们

● 一个普通的本科院校

● 一个最普通的讲师和信息安全技术学习者

● 一群热情、坚持的同学们



我们的团队



热情
坚持

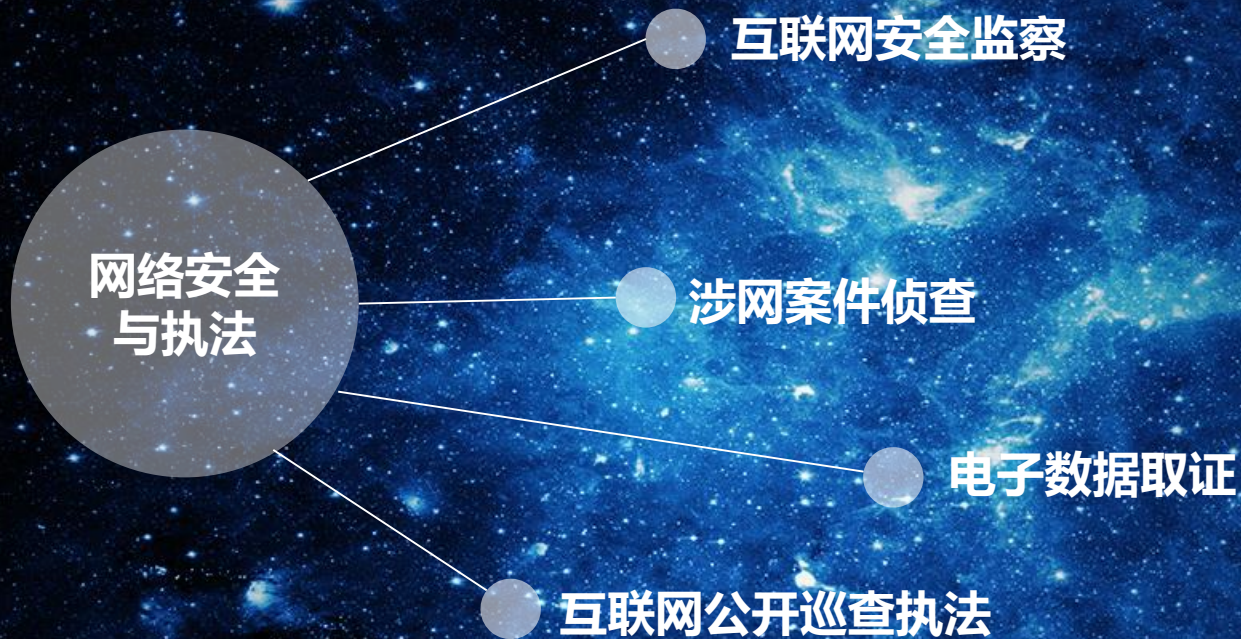
团结
创新 奋斗



网络空间安全新常态



网络安全保卫



那些传奇



tombkeeper
于旻



袁哥
袁仁广



heige
周景平



余弦
钟晨鸣

.....

那些传奇

信安人才的标准？
信安人才是教不出来的？
北向人才？南向人才？

理想与现实

学校教育：体系的、严谨的、基础的、理论的

实践需求：解决问题为导向

WHY? 课程设置? 培养目标? 实践环境? 考核机制? 校企合作? 创新精神?

论一个教师的自我修养

互联网+教育：机遇与挑战

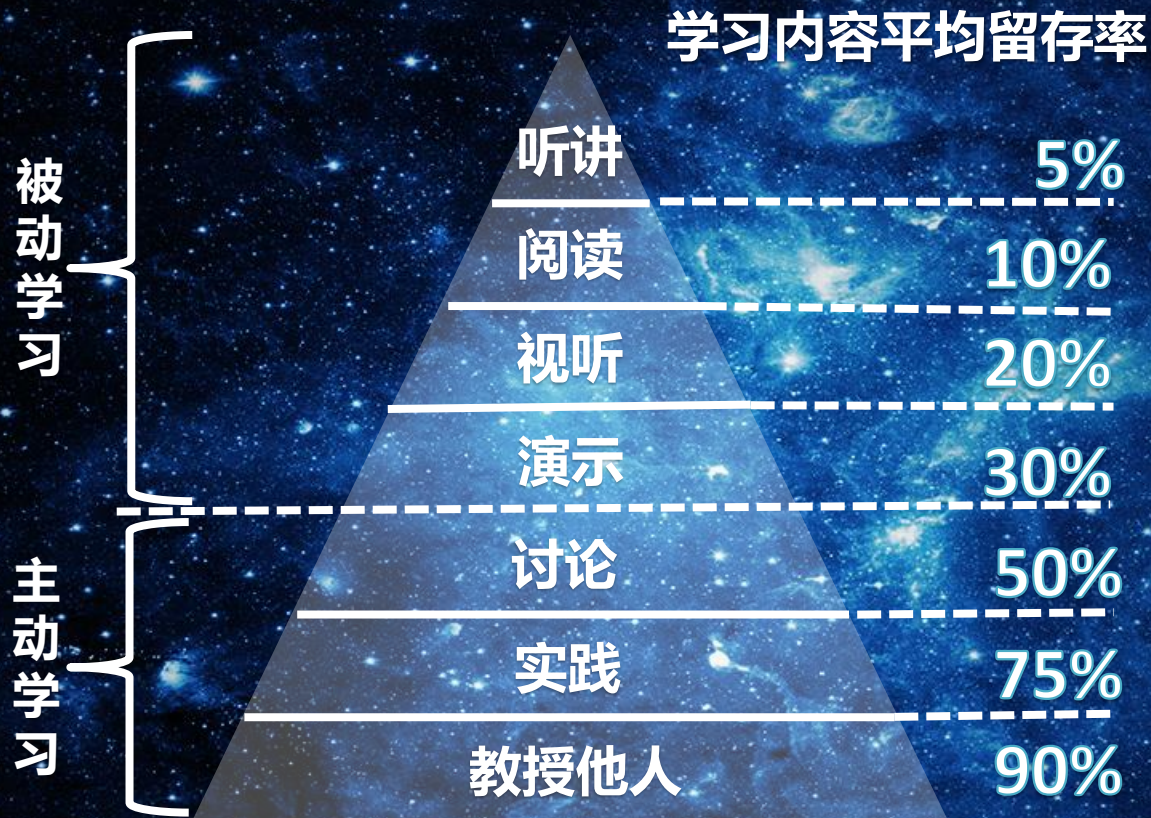
学习
途径

MOOC 微课 在线实验平台 社群.....

角色
转换

教师：讲授者到学习组织者

论一个教师的自我修养



论一个教师的自我修养

打通学校教育与实践任督二脉的关键一环：教师



论一个教师的自我修养

夯实基础



培养兴趣



扩展思路



引导提高

授人以鱼不如授人以渔
信息安全的知识、技能、理念的渗透

我认识的新生代

优点

与生俱来的互联网思维
爱炫、喜欢有趣的事
开放、平等、共享
创造力

.....

缺点

同优点

信安团队培育

兴趣使然，志同道合



带队老师的作用：“后勤保障”、“指南针”、“外联宣传”、“技术咨询”、“法律顾问”、“知心阿姨（叔）”

成长型信安团队

- 成立时间较短，文化积淀少
- 技术尚处在积累阶段
- 团队成员技术路线分布不均衡
- 外部资源与内部支持较少

成长型信安团队



万事开头难

与各位小朋友们分享入门之道

职业规划 美国网络空间安全教育计划 (NICE)

技能指引 知道创宇研发技能表

竞赛切入 MISC, PPC, CRYPTO, PWN, REVERSE, WEB, STEGA

众测平台、SRC 未经授权的渗透测试是非法行为!!!!

在线实验平台 合天、i春秋、白帽学院、西普.....

以竞赛促发展

按竞赛类型分：

应用作品提交类

论文提交类

攻防对抗类：CTF竞赛

以竞赛促发展



荣誉感

成就感

团队精神

技能提升

CTF之我见

寓教于乐
锻炼思维
训练技能

进一步宣传普及
避免过度的娱乐化
贴近实战
给新人一定的发展空间

莫忘初心

路漫漫其修远兮

- 明确的短期目标
- 考核机制
- 退出机制
- 老带新持续学习的氛围

SDPC-网安-训练

时间	授课人	授课计划	校内比赛要求	CTF时间表:	附:
开学周 2.29-3.6	无	准备比赛	1-统一采用ctfd平台进行搭建, 自己自行搭建	SSCTF 2016 初赛 二月 27, 2016, 8 a.m. — 二月 29, 2016, 8 a.m. OCTF 2016 初赛 三月 12, 2016, 8 a.m. — 三月 14, 2016, 8 a.m BCTF 2016 三月 19, 2016, VolgaCTF 2016 Quals 25 三月 2016, 15:00 UTC — 27 三月 2016, 15:00 UTC Nuit du Hack CTF Quals 2016 01 四月 2016, 21:59 UTC — 02 四月 2016, 21:59 UTC BlazeCTF 2016 20 四月 2016, 04:20 UTC — 24 四月 2016, 04:20 UTC 360GeekGame时间待定 CUIT校赛时间待定 东南大学CTF时间待定 ISCC 五月 1,2016-五月 31,2016 (重要, 大二争取全部进入线下赛决赛)	1-期间可能会有一些比赛次数来解决 2-微信公众号的信息 3-社团淘汰制度开学 4-机房内不得玩游戏, 讨论, 开学就改, 打比赛 5-因为下学期机房与宿舍定, 周六一般晚上才有 6-大一人员参加CTF比赛 360Geek game、东南大学其余比赛大二参加, 7-周一至周五其余时间材料
第一周 3.7-3.13	袁心宇	burpsuite入门			
第二周 3.14-3.20	刘家希	逆向破解1	2-题目为所有人共同出题		
第三周 3.21-3.27	王晓栋	wireshark入门			
第四周 3.28-4.3	袁心宇	sqlmap入门	3-比赛结束后负责人进行ppt讲解		
第五周 4.4-4.10	刘家希	逆向破解2			
第六周 4.11-4.17	王晓栋	环境搭建与简单的web测试	负责人 王晓栋、刘家希		
第七周 4.18-4.24	刘家希	逆向破解3			
第八周 4.25-5.1	王晓栋				
五月一整月	ISCC				

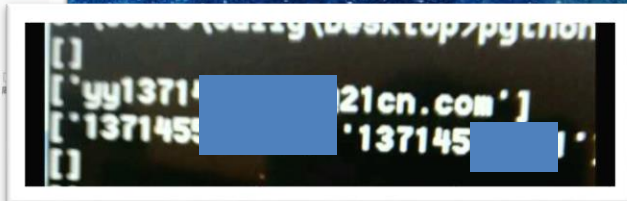
每次校内结束比赛的那个周六进行例会, 例会内容主要为:

- 1-社团培训计划
- 2-一些需要改进的现象

从实践中来到实践中去

- 安卓恶意代码分析
- 伪基站数据分析
- 钓鱼网站调查

1 1457488659 460021547946095	2016-03-09 10:00:48 460021547946095
2 1457488659 460021547946095	2016-03-09 10:04:21 460021547946095
3 1457488659 460020657911733	2016-03-09 09:57:39 460020657911733
4 1457488659 460020657911733	2016-03-09 10:00:48 460020657911733
5 1457488659 460020657911733	2016-03-09 09:57:39 460020657911733
6 1457488659 460028637012054	2016-03-09 09:57:39 460028637012054
7 1457488659 460028637012054	2016-03-09 09:57:39 460028637012054
8 1457488659 460021637034342	2016-03-09 09:57:39 460021637034342
9 1457488659 46000490652884	2016-03-09 09:57:39 46000490652884
10 1457488659 460022637026503	2016-03-09 09:57:39 460022637026503
11 1457488659 460078537503647	2016-03-09 10:00:48 460078537503647
12 1457488659 460009421343245	2016-03-09 09:57:39 460009421343245
13 1457488659 460028637012054	2016-03-09 10:00:48 460028637012054
14 1457488659 460078537503647	2016-03-09 10:04:21 460078537503647
15 1457488659 460021637034342	2016-03-09 10:00:48 460021637034342
16 1457488659 460009421343245	2016-03-09 10:00:48 460009421343245
17 1457488659 460028637012054	2016-03-09 10:04:21 460028637012054
18 1457488659 460022637026503	2016-03-09 10:00:48 460022637026503
19 1457488659 460021637034342	2016-03-09 10:04:21 460021637034342
20 1457488659 460009421343245	2016-03-09 10:04:21 460009421343245
21 1457488659 460022637026503	2016-03-09 10:04:21 460022637026503
22 1457488659 46000490652884	2016-03-09 10:04:21 46000490652884
23 1457488659 460025547475936	2016-03-09 09:57:39 460025547475936
24 1457488659 460003790652883	2016-03-09 09:57:39 460003790652883
25 1457488659 460025547475936	2016-03-09 09:57:39 460025547475936
26 1457488659 460021547946095	2016-03-09 10:00:48 460021547946095
27 1457488659 46000490652884	2016-03-09 10:00:48 46000490652884
28 1457488659 460025547475936	2016-03-09 10:00:48 460025547475936
29 1457488659 460003790652883	2016-03-09 10:00:48 460003790652883
30 1457488659 460021547946095	2016-03-09 10:04:21 460021547946095



针对建行伪基站诈骗信息的分析以及实际渗透

2015-10-10 山警网安 山警网安安全实验室



问题与困惑

现实问题：

教学效果评价体系

科研、教学基本工作量的压力

社团活动资金支持

师资培训问题

学生升学就业政策问题

解决之道

放下功利

**警学企研的协同创新：
在教师、安全专家、执法人员和检察官
之间架起沟通的桥梁**

寻梦?撑一支长篙,
向青草更青处漫溯;
满载一船星辉,
在星辉斑斓里放歌.

Thanks !
好客山东欢迎您！

