



破解企业攻防实战人才 缺失的困境

张兆心

哈尔滨工业大学(威海)
网络与信息安全技术研究中心(NIST)

求真 奋进 务实 创新

需求

- 可快速上手了解业务系统的人才
- 保障企业安全的人才

困境

- 供需不匹配
漏洞挖掘人员or攻防实战人才
- 培养代价非常大

解决方案

- 寻找具有漏洞挖掘能力的人
- 试图培养真正的需求点

人才能力培养很重要

能力如何转为生产力更需要进行大量探索

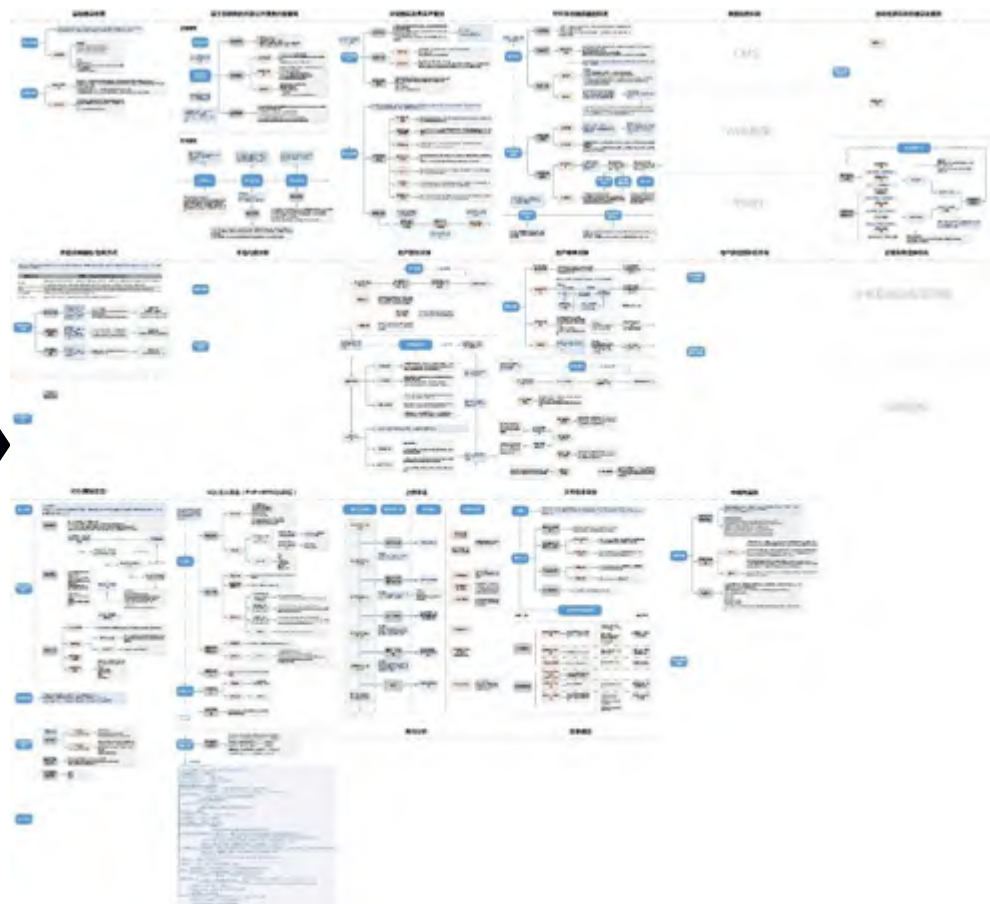
攻防实战型人才定位



实战出发、攻防兼备

完整的知识体系

漏洞成因的深入理解



学生攻防技术培训实践



课程效果反馈

- 兴趣极高
- 非常关注后续进展
- 钻研性强



学生客观特点

- 无业务概念，基础差
- 无体系支持
- 专注
- 可塑性强

针对问题做出的尝试



培训方法:

- 根据漏洞原理及防护方案建立攻防技术体系
- 建设实验平台以实现实践环境

培训方式:

- 建立大一“直培”体系
- 寒暑假封闭集训

培训环境:







































- 配套教材
- 具备实际经验的讲师



Web 安全防护概论

从代码层面了解安全漏洞本质
防护手段的应用

有效培训手段汇总

 utf-7绕过实体化编码 (仅IE可用, 测试环境)	 2	 CSRF
 XSS_payload	 3	 include
 跨站脚本攻击-20150807-10.docx	 4	 middleware
 快速测试-xss篇-刘骁睿_160424.docx	 5	 other
 从代码中看XSS_余超_160327.docx	 Ret2addr	 RCE
 框架防御SQL注入_余超_160408.docx	 Ret2reg	 sql
 用户管理逻辑_余超_160426.docx	 linux-exploit(1).docx	 SSRF
 MySQL安全配置_向凌召_160420.docx	 linux-exploit(2).docx	 upload
 php大括号特殊用法总结.docx	 linux-exploit(3).docx	 Web木马
 php弱类型整理_卢童_160328.docx	 linux-exploit(4).docx	 xss
 利用pkav实现对验证码的识别.docx	 linux-exploit(5).docx	 代码审计
 西普学苑ct知识点整理 (web篇)_李思	 linux-exploit脚本编写教程.docx	 信息收集
	 paperFor4.9.pptx	 业务逻辑

CVE-2016-1494 (python – rsa)漏洞详解

uncleheart 2016-04-12 共155865人围观, 发现7个不明物体 系统安全 终端安全

原创作者: uncleheart

0x01 概述

[CVE-2016-1494](#)漏洞讲的是Python-rsa的签名伪造。在某些特定情况下, 可以伪造python rsa库生成的签名信息。但是前提需要RSA的公钥指数e值很小, 以下皆以e=3讨论。

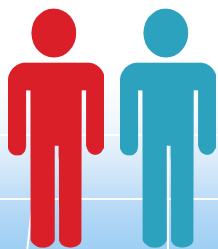
人员基本能力

- 可直接利用的攻防知识体系
- 漏洞的综合分析能力
- 代码审计能力

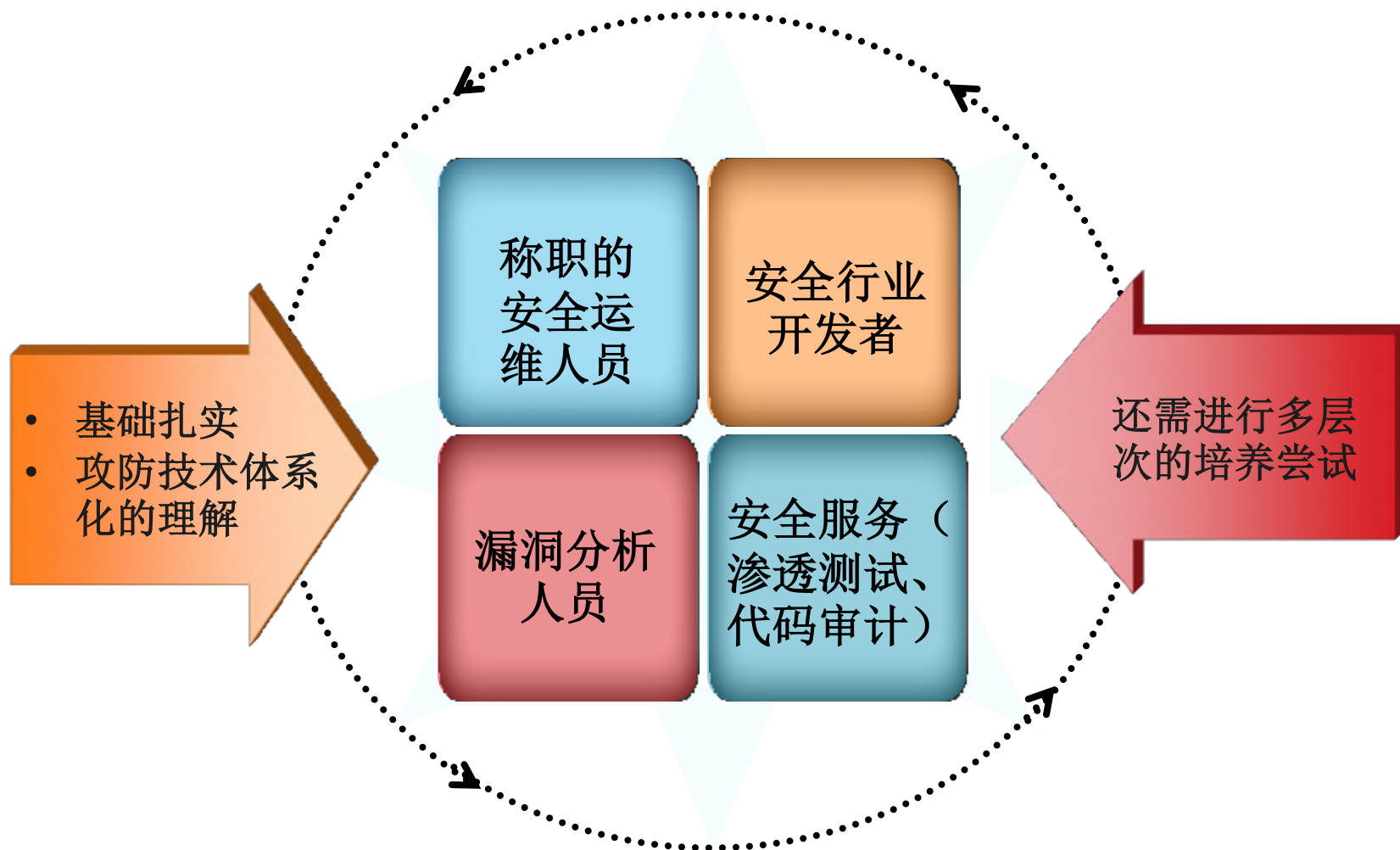
攻防实战经验

- Web漏洞挖掘
- 逆向技术
- 内网渗透
- 病毒分析
- ...

效果



人员能力判定标准缺失



A set of keys is shown, including a large metal key, a smaller key, and a keychain with a white tag. The keys are resting on a light-colored, textured surface. The lighting is soft, creating a slight shadow to the left of the keys.

Thanks!