信息安全整体保障中的漏洞挖掘

演讲人：蔚永强 2019.3.1

我是谁、我来自哪、我是干什么的？

- 我是蔚（yù）永强；
- 现就职于成都卫士通信息产业股份有限公司高级安全专家职位；
- 工作十一年，从事信息安全行业时间七年，服务过上百家单位，经验异常丰富；
- 现主要负责中国电子科技集团旗下五百家成员单位的信息安全工作以及大型央企的信息安全整体保障服务工作；
- 经常活跃于各大安全应急响应中心进行漏洞/情报提交，多次获得特殊奖励。

成都卫士通信息产业股份有限公司

- 国内第一家信息安全上市企业（股票代码：002268）；
- 国内知名密码产品、网络安全产品、互联网安全运营、行业安全解决方案提供商；
- 首批商密产品研发、生产、销售资质单位；
- 首批涉密信息系统集成甲级资质单位；
- 参与国家信息安全蓝图设计，引领信息安全核心技术发展，承担大量国家科研创新项目，拥有完整的信息安全产业链。

什么是信息安全整体保障服务

信息安全整体保障服务主要面向大型企业提供的一种全方位的信息安全服务，将网络信息安全规划、安全评估、安全设计、建设实施、安全运维、安全培训及人才培养等全生命周期安全保障过程统一纳入到安全服务范畴，为企业构建网络安全管控、安全防护、安全服务三大体系化的网络信息安全保障能力，提供“全托管”、“一站式”网络信息安全服务。

招商局集团

- 特大型国有央企
- 注册资本168亿人民币
- 总资产8万亿人民币
- 2018年世界500强280位

中国远洋海运集团

- 特大型国有央企
- 注册资本110亿人民币
- 总资产6100亿人民币
- 2018年世界500强335位

漏洞挖掘路上遇到的问题

信息安全整体保障中漏洞挖掘遇到的问题

- 信息收集（不清楚客户业务系统架构，完全黑盒测试，两眼一抹黑）
- 登录问题（业务系统采用UKEY、证书、IE控件等方式进行登录）
- 密码问题（业务系统已经对弱密码用户进行强制修改）
- 统一登录（业务系统采用了统一身份登录平台进行身份验证进行验证）
- 二次校验（业务系统密码对了，发现还存在二次验证）
- 防护问题（业务系统前端存在云WAF防护或内网部署了下一代防火墙设备）
- 反弹问题（业务系统无法反弹SHELL，内网主机无法上网）
- 代理问题（业务系统代理无法正常工作，内网主机无法上网）
- 知识问题（发现知识面不够广，导致漏洞挖掘的姿势不够多）
- 工具问题（常用的工具已经无法满足挖洞的需求，需要自己动手写利用工具）
- 安全测试（业务系统已经经过多次安全测试，并进行了相关漏洞修复）
- 封杀问题（刚发现点问题，发现网络出口被封杀了）

信息安全整体保障中漏洞挖掘的解决思路

- 工具集合（抓包分析类、漏洞利用类、逆向分析类、模糊测试类、代码审计类）
- 收集信息（系统架构、安全防护、信息资产、公司架构、员工信息、托管平台、威胁情报）
- 信息整理（将收集的目标信息进行整理分析，输出高质量测试内容）
- 目标选定（从最易目标进行漏洞挖掘，然后对难目标进行漏洞挖掘）
- 测试方式（对测试点要采取多种方式进行漏洞测试，不要丢弃看似风险较低的漏洞）
- 团队力量（要有一个团队，遇到问题时，虚心接受团队人员给予的建议以及帮助）
- 知识积累（漏洞挖掘中每一个新的发现，都是一次知识的积累，要做好记录）
- 心态调整（每一个人都会存在心理上的问题，无法坚持、容易放弃，其实你离成功只有一步之遥）
- 方法细节（细节是每一个请求、响应、代码逻辑，方法是每一个漏洞利用，方法与细节即是武功秘笈）
- 尖刀作战（在挖洞过程中，尖刀作战是很重要的，但不是人越多越好，不然容易暴露哦！）
- 漏洞提交（嗯？干嘛呢兄弟，想好下一个漏洞咋挖了吗？想好了再提交，呵呵！）
- 漏洞重审（你以为挖洞完事了？挖不着了？变换思路，“回首，掏！”）
- 挖洞复盘（要设定目标，并在最后阶段对整个过程进行复盘整理）

阿宝的性格决定了"他"的命运

- 从底层工作做起，能吃苦耐劳，能吃，身体好。
- 有理想、确定目标、付诸行动、勤于练习。
- 领悟能力、学习能力超强，有一个非常厉害的师父。
- 为"人"正直、可靠、团结，有一个非常棒的团队。
- 为"人"幽默、外向、亲和力十足，善于与别人交流。
- 不屈不挠、越挫越勇、不放弃，有一个强大的内心。
- 由不自信到成为功夫大师，能努力改变自己的命运。
- 成为大师后，一如既往、不骄不躁、不摆架子。

大师性格

安全忠告

漏洞千万条，安全第一条。

漏洞要提交，做个好白帽。

协议要遵守，奖励少不了。

挖洞不规范，**跑不掉。

THANKS