登录

黑客之死

破天 / 2017-09-19 03:12:51 / 浏览数 4619 安全技术 技术讨论 顶(0) 踩(0)

开篇之前，先介绍一下自己的职场经历和安全行业经历，并无意抨击或贬低任何一种安全从业人员。仅对最近两年安全圈或者黑客圈、白帽子圈发表一下自己的看法。

08年因为《魔域》账号的丢失，想着怎么找回，后来发现找回无望，又想着弄明白怎么盗号，后来又想弄明白怎么才能不被盗号，就这样一条线拉着一条线，慢慢把我
白帽子啥的，黑客并无贬义），上面说安全圈，干脆叫黑客圈，为什么这样说？理由很简单，当时安全人员没地方吃饭，没有就业岗位，只能求其次选择了除了安全更擅长的

在这个大环境下，我经历了金融服务商（两年）、老牌国企金融机构（六年）、互联网金融机构、大型互联网机构。在金融服务商，把安全概念带进了机房和客户服务，在金

“安全圈现在就是娱乐圈”，最近两三年最直观的感受，哗众取宠，争强好胜，甚至以斗图、互怼、肉鸡量、shell量等等来炫耀，我不知道这样对不对，可这不是我印象里

第一代黑客

1、综合素质强，安全设备、安全研发、数据库、系统、应用、中间件、业务系统、语言、网络架构、系统规划建设等颇有涉猎

2、懂得针对业务特点、企业实际环境设计符合现状的安全体系架构和安全技术架构

3、有格局，有技术，有管理能力和个人资源。

4、对各大厂商的产品、技术甚至商务都如数家珍

第二代黑客，

1、绝大数从事安全相关工作，一部分身兼数岗，网络和安全、运维和安全

2、熟悉常见系统架构和风险

3、多年从业有自己的认识，但缺少对系统性的理解。

4、可以负责安全团队的部分内容。

第三代黑客

1、 挖洞

2、 挖洞

3、 挖洞

4、 缺少专业知识和系统化概念

5、 爱好混迹各种沙龙

6、 擅长斗图、getshell、各种互联网找洞。

7、 职业规划不明确，自身定位价值偏差

个人的浅见，三代黑客代表了中国三代黑客文化，更代表了必不可少的黑客成长历程，从挖洞入门，通过沙龙交流学习，缺少的专业知识通过各种充电来提升，成长为安全团

在乌云笼罩的日子，一个帖子如果不能有绝对的干货，一定会被pass，一个漏洞提交，如果详细度不足以让审帖人员顺利复现，一定会被pass，厂商多久不修复，一定会被

中国的网络安全法，成立于2017年6月1日，说明我们的安全开始被国家重视，虽然现在被很多人说“贵圈很乱”，我想只是因为我们还小，我们需要成长，更需要良好的

1、安全不只是挖洞，甚至挖洞在乙方的工作量都占不到一般，更遑论甲方。

2、不要那么浮躁，静下心学些真正的安全技术。

3、多写点东西总没错，安全本就是综合性的能力。

4、进入安全圈，不是认识几个人，参加几次沙龙、提交几个漏洞、写过几篇挖洞或者工具利用的文章。

针对社会白帽子和企业安全员，也针对挖洞和企业安全阐述一点自己的看法：

1、挖洞，现在大家停留在最基础的逻辑洞、通用洞或NDAY漏洞上，去互联网扫公网IP，比如strust2 045
052等，用工具一扫一堆，这些漏洞真的有价值吗？有，但还不够，如果把漏洞发现和漏洞简单修复，上升到架构设计规范、上升到安全标准体系、上升到通用安全基线是不

2、企业安全，企业安全按企业类型划分为，传统企业安全、互联网企业安全，企业安全涵盖了五大领域基本包括网络安全、业务安全、安全体系建设、风控合规及审计、业

信息安全管理：制度、流程 整体策略等

基础架构与网络安全：制度、流程 整体策略等

基础架构与网络安全：IDC\生产网络的各种链路、设备服务器、服务端程序、中间件、DB，漏扫 补丁修复 ACL 安全配置 N/H ips等

应用与交付安全：对各BG、业务的产品进行应用级风险评估 代码审计 渗透测试 代码框架的安全功能和应用级防火墙、IPS等，包括SDL等

业务安全：账号安全 交易风控 征信 反价格爬虫 反作弊饭bot程序 反欺诈 反钓鱼 反垃圾信息 舆情监控 防外挂 打击黑产 安全情报 态势感知等

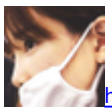
企业认证和合规标准：等级保护测评认证、国内的ISO2700x、国外的BS7799和BS25999等

企业级安全管理：战略级安全规划建设、安全预算、TCO/ROI等

作为黑客的你，看完上面的内容还觉得挖洞只能做到这样了吗？除了挖洞我们真的没得做了吗？

上一篇：XSS思维导图 下一篇：FFmpeg RTMP Heap ...

1. 5 条回复


hades 2017-09-19 03:21:44

一直觉得搞二进制的比web的稳的多

0 回复Ta


monika 2017-09-19 03:35:53

第三代黑客

1、 挖洞

2、 挖洞

3、 挖洞

4、 缺少专业知识和系统化概念

5、 爱好混迹各种沙龙

6、 擅长斗图、getshell、各种互联网找洞。

7、 职业规划不明确，自身定位价值偏差

个人的浅见，三代黑客代表了中国三代黑客文化，更代表了必不可少的黑客成长历程，从挖洞入门，通过沙龙交流学习，缺少的专业知识通过各种充电来提升，成长为安

在乌云笼罩的日子，一个帖子如果不能有绝对的干货，一定会被pass，一个漏洞提交，如果详细度不足以让审帖人员顺利复现，一定会被pass，厂商多久不修复，一定会

 中国的网络安全法，成立于2017年6月1日，说明我们的安全开始被国家重视，虽然现在被很多人说“贵圈很乱”，我想只是因为我们还小，我们需要成长，更需要良好

0 回复Ta

cover 2017-09-19 06:29:04

站得高，望得低

0 回复Ta

 2017-09-19 10:10:55

I can't agree with you more.

0 回复Ta

b5mali4 2017-09-19 10:22:26

很真实吧，现在很多人的确只是挖洞挖洞，天天特别喜欢做那种1+1=2的东西。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录