0x01 企业安全测试

什么是渗透测试？

通过真实模拟黑客行为、分析方法来对系统进行模拟攻击测试。

常见的安全测试模式有哪些？

传统渗透测试、众测、自建SRC（应急响应中心）。

0x02 传统渗透测试

传统意义上的渗透测试服务会尝试验证每一个漏洞的威胁，并帮助用户真正理解漏洞的成因，做到自己可以控制自己可以防御。每一次渗透测试都由安全专家手动实施，测试完成后，还会提出专业修复建议，帮助真正解决安全问题。

优缺点？

企业想做渗透测试，一般是会找一些安全厂商，沟通需求，明确测试范围。

安全厂商为企业提供透测试服务，能够提供现场技术支持，场景可控，人员可控。

但企业根本不了解安全服务公司最终会派什么水平的渗透测试人员给企业信息系统进行渗透测试检测，不同水平的人，企业所需要支付的费用也都相同。

甲方过于相信乙方的安全能力，而造成了"这个目标已经做过渗透测试了为什么还会出问题"这样的疑问出现。

0x03 安全众测

什么是众测?

所谓众测，就是众包模式在安全测试领域的一种表现。也就是企业把自己的产品给到安全众测平台，由平台的安全人员(这些安全人员也不隶属平台，而是来自互联网)进行安全测试。

众测其精华在于"众"，测试人员够多，群测群力，不论是从广度还是深度上来说，能够更全面地去发现更多问题。

众测优点

我们将众测来和以往的渗透测试做个对比。传统的渗透测试模式中，1-2名测试人员，花费5天的时间，有时只能帮企业找出一个高危漏洞，而企业往往要花费高达10万元的渗透测试费用。在传统的渗透测试模式中，全部是按照人天进行计费，安全公司虽然会派出资深的安全专家，但由于测试人员少，没有竞争，测试的广度与全面程度必然受到限制，发现的问题往往不够全面，很多掩藏的问题，在上线之后才慢慢浮现，带来更大的损失。

而悬赏式、项目式的众测，企业往往能规定自己的测试范围，挑选自己的测试人员，专业的厂商和白帽子们会在奖励和竞争的驱动下，发挥出更大的功力。

众测弊端

现在市面上的众测平台已有多家，其中很多众测平台都是选取互联网上的测试人员来进行测试，导致测试的人员不可控，测试的结果存在很大的不确定性，测试过程中所带来的安全风险不可控。

怎样选择出最可靠的可信众测平台

选择众测平台的时候，不要只问："能帮我找出多少个漏洞"；更要问问："你们的测试人员从哪里来？如何管理？"

平台私密、人员可靠、协议授权、规定范围、相互信任。

目前为止，众测仍然是全球范围内，性价比最高、效果最好的安全测试模式。

三大众测服务平台：

补天众测：https://butian.360.cn

先知众测：https://xianzhi.aliyun.com

漏洞盒子：https://www.vulbox.com

白帽子奖励计划：

应用类型	严重	高危	中危	低危
核心应用系统	5400-6000	3000-4000	800-1200	60-200
一般应用系统	2000-3000	1200-1800	600-800	30-100
边缘应用系统	600-1000	300-500	100-200	10-50

0x04 应急响应中心

很多企业都建立了自己的安全应急响应中心（SRC），搭建企业和白帽子之间的桥梁。

补天漏洞响应平台推出了托管式安全应急响应中心V2.0版本，参考链接：https://butian.360.cn/Service/pri。

未来，将会有更多的企业去建立自己的安全应急响应中心（SRC）。

0x05 总结

本文通过介绍几种安全测试模式，进行综合对比，如下：

安全测试模式	传统渗透测试	众测	自建SRC（应急响应中心）
测试人员	水平参差不齐	群测群力	群测群力
项目成本	性价比低	性价比高	运营成本高
项目场景	测试场景可控	漏洞收集范围大，不可控	漏洞收集范围大，不可控

另外，现在的攻击者更倾向于利用业务逻辑层的应用安全问题，这类问题往往危害巨大，可能造成企业的资产损失和名誉受损，并且传统的安全防御设备和措施收效甚微。

漏洞认定问题：在业务逻辑漏洞认定过程中，可能会存在一些偏差，比如某系统存在业务逻辑漏洞，偏离了原来的设计初衷，乙方认为是高危漏洞，但甲方认为该问题为产品策略设定，甲方允许这样的业务逻辑存在，评价中危。

关于安全测试的一些思考：

1、不论是传统渗透还是众测，有测试环境的，使用测试环境进行测试；

2、A+B模式：互联网系统优先考虑使用众测，内部系统（或特定场景下的系统）考虑安全厂商提供的渗透服务。

3、安全的主动权牢牢抓在甲方手里，不过分依赖乙方的安全能力。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。