安全小课堂第六十五期【日志审计与网络安全】

京东安全应急响应中心 2017-07-14

日志审计是常见的一种审查网络安全威胁的方式，并且，随着大数据安全的兴起，日志审计与大数据相关技术结合是一种新趋势。JSRC **安全小课堂第六十五期**，邀请两位老师分享日志审计与网络安全那些事，本期小课堂邀请到了**关中大侠**、**lion**老师进行分享,同时感谢JSRC白帽子们的精彩讨论。

简述日志审计对网络安全的重要性？

京安小妹

首先日志是一个系统中很重要的一部分,正常情况下可以通过日志进行错误排查，作为性能优化的参考等。
在安全方面，可以发现一些异常的行为，比如频繁的登录失败、不正常的URL请求等等；
很多的蛛丝马迹 都可以从日志里边看出来。

讲师： lion、关中大侠

日志审计能主要审计内容（网络安全方面）有哪些？

京安小妹

其实主要是说的6个W Who When How What Where Why 。
一个事情的几个要素可以归结为：时间、地点、人物、起因、经过、结果；
那么对应一条日志：时间、IP、username、url、操作内容、成功失败；
其实就是看谁在什么时间，干了什么，他为什么要这么做。
发现了对手的水平，动机 ，基于这个来往下看的话，其实就很简单了。

讲师： lion、关中大侠

日志审计在加固网络安全方面的效果如何？

京安小妹

攻击的定位，事件的溯源，以及事后的casestudy，都是通过各种日志说话。
在事中的时候 ，可以看到哪里正在被攻击 ，从而进行防御例如最暴力的封ip,而在事后如果重新审计日志，那么可以总结一下自己的不足，另外重要的一点是看看 哪里沦陷了。或者说，受到的影响范围都有哪些 。

讲师： lion、关中大侠

在搭建日志审计体系可能遇到的问题有哪些，如何解决呢？

京安小妹

1、日志格式不统一
解决方法:这个是硬伤,只能去协调了。
2、日志源的问题
解决方法一:是流量镜像,这样的好处就是基本上不用弄太多的agent。
解决方法二:就是各种服务器接收日志,这样的工作量来说比较大 。
3、日志太大怎么分析
解决方法:志量太大，存储 ，分析 ，筛选 这些，对于日志系统来说，都会有比较大的考验。
4、rsyslog发送大量日志的时候，采用TCP导致过一次运维故障
解决方法:所以现在rsyslog全部都改为udp了，前提要保证网络的稳定性。

讲师： lion、关中大侠

白帽子提问:收集日志过程中，如何判断client日志的agent是正常传输日志的，而不是出现假死导致日志可用性出现问题?

这个最好的办法就是监控了就是如果一段时间没有收到流量 或者流量在正常时间的情况下出现比平时少那么就报警。

讲师： lion、关中大侠

白帽子提问:那你们在日志分析的时候，有没有分析过代理运营商的攻击行为，这种出口IP一般对应一个大的内网，你们怎么溯源抓人？

这种情况是有的 ，不过暂时我们还没抓人 ，不过可以通过其他的手段 ，非IP 的手段来找到人的。

讲师： lion、关中大侠

是否有关于日志审计的工具推荐？

京安小妹

elk现在这个用的最顺手了。
其次是splunk。

讲师： lion、关中大侠

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文

阅读原文