

服务器安全管控的探讨——安全小课堂第十三期

京东安全应急响应中心 2016-06-03

安全小课堂第十三期

作为网络的核心产品，服务器技术相对复杂，尤其是在病毒肆虐的网络时代，安全问题显得更加突出。本期我们来聊一聊服务器的安全管控。

本期邀请到了万达电商安全专家林鹏、唯品会安全专家向坤，还有京东信息安全团队的李艳勋，来和大家探讨交流哟~□□□

12



豌豆妹

请问服务器安全管控面临哪些风险呢？



葫芦娃

Windows服务器已经不是主流，我们今天可以着重聊聊Linux方面。



哆啦A梦

那我就先来抛个板砖吧。从安全性考虑，那必然是防止服务器被入侵，从广义的安全三要素来说，保证服务器的可用性，其实也算是服务器安全管控的一个标准，不过现在这块其实跟运维也有点关系，所以，目前大部分的安全部门，是不太会介入这个方面的管控。

小新



简单列举下吧，以下都可能造成服务器账号被口令爆破、通过web漏洞上传webshell等途径被拿到主机权限：1、主机运行的网络服务没有安全评估、加固；2、开源软件、框架存在的通用漏洞；3、开发人员没有足够的安全编码意识等。简单来说，就是**技术安全+管理安全风险**。



豌豆妹

那服务器安全管控应该注意什么呢？



小丸子

我觉得，首先是建立一个服务器的行为安全基线，这个是判断服务器有没有异常行为的重要标准，我现在的思路就是找出异常的模式，当然这个异常的行为，就是需要一个尺度，也就是用基线去衡量。**没有这个基线的话，很多东西，都没法去判断**，例如每天服务器的登录情况，文件的变化情况，网络的流量情况等，都需要一个基线。



哆啦A梦

举双手同意。服务器的行为安全基线是Linux服务器安全的基础。没有这个，后面的管控技术和管理手段都是没有办法落地的。当然，**这个应该也是比较难做的事情，需要一个积累的过程，其实挺枯燥**。

2



豌豆妹

大家能谈谈HIDS和NIDS的区别么？

葫芦娃



HIDS 就是主机IDS，主要负责监控主机的情况，比如主机的文件变化，端口开放情况，本机的网络连接情况，与本机相关的本地操作等，顾名思义，主要侧重点就是主机。

NIDS，网络IDS，侧重点是网络。主要负责的就是对网络中的流量进行分析。NIDS因为具有网络分析能力2层以上的包都能解开，因此可以发现很多网络的攻击，最简单的可以基于网络中的流量包里的关键字进行检测。HIDS是横向扩展的，NIDS有性能瓶颈。

小新



有很多互联网公司，在自研HIDS，需求也是定制化的，HIDS检测的安全风险主要包括发现黑客入侵行为、检测Trojans/rootkit/backdoor、服务器安全漏洞检测等等。在理想情况下，HIDS可以发现一切主机被入侵的行为，当然，这只是在理想的情况下。

3

豌豆妹



HIDS能发现哪些安全风险呢？

葫芦娃



就拿OSSEC来说，可以通过文件变化情况，发现webshell，可以通过端口变化，发现

反射后门，当然还可以通过使用OSSEC的针对syslog或者自定义的log发现其他的行为，例如暴力破解账号，IP异常登陆等等。



豌豆妹

HIDS在互联网企业的应用多吗？



小丸子

在大的互联网公司刚需，而且在支付牌照申请、合规检测等场景中也是有明确要求的，目前，主流的云厂商也都提供了HIDS防护产品，很多公司的HIDS功能，可能是和其他一些运维监控系统整合在一起的。



葫芦娃

我个人觉得，用的人不多。HIDS需要非常有经验的人去部署策略，所以使用的企业应该不多，而且若因为设置的不好，反而会产生大量的误报。

4



豌豆妹

那服务器安全的配置工具有哪些呢？有好用的推荐么？



哆啦A梦

入门级的可以用安全狗、青藤，Windows和Linux都支持，可以一定程度提高攻击门

槛，但不能 100% 防御。自动化的产品主要是一些商业产品，比如 <http://www.tripwire.com/>，趋势、McAfee等几个大的安全厂商都有。互联网企业的加固脚本估计都是自己写的吧。□

5



豌豆妹

企业级Web服务器安全该怎么做呢？



小丸子

现在我们在尝试或者已经在做的事情，比如账号密码的统一管理（PIM），主机HIDS对主机的行为、配置、入侵进行检测和监控，服务器上线前的基线检查和加固，定期的服务器基线检查和安全扫描，HIDS日志需要发送到SOC进行监控和审计等等。



哆啦A梦

服务器安全的保障，应当加强运维/开发人员的安全意识、实施主机加固策略、建立安权监控/检测机制。这是一个比较大的话题，涉及技术、管理；网络、主机、应用不同层面的保护、检测。例如，1、设计并完善网络安全域划分结构，实施安全域划分；2、严格限定应用程序的执行权限；3、主机安全加固：包括账号口令策略、iptables策略限定对外开放的服务及访问约束；4、对服务器操作日志记录、审计；5、对入侵主机事件的检测手段，主机安全扫描等等。



小新

唔，还有个流程的事情，其实我觉得也挺重要的。是这样的，之前我申请了一个服务

器，通过了流程完成了申请，服务器分配。后来我拿到了IP地址，口头告诉了我们的一个同事，那个同事根据我说的IP，登陆了服务器，格了硬盘，我想了一下，如果万一，我IP说错了，比如ip最后一位是121，我告诉他是21，就是少看了一个1，那么就会出现严重的后果，所以想到这里，觉得有点后怕，希望大家不要掉这个坑里。



豌豆妹

是的，**流程上需要两人确认**。还有就是换硬盘，也会有类似的隐患。



葫芦娃

就上述事故，在云化的环境里面，在自动化的运维交付中就可以缓解。之前我参与过一个私有云落地的项目，运维就明确要求交付自动化。所有的image、软件、配置、策略、交付流程完全控制起来。这样也会杜绝我们之前提到的一部分问题，这个其实对安全也有很大的帮助。



豌豆妹

哈~听君一些话，胜读十年书，受益匪浅呢~感谢大家的热烈参与~咱们下期见哟~



安全小课堂往期回顾：

- 1、论安全响应中心的初衷；
- 2、安全应急响应中心之威胁情报探索；
- 3、论安全漏洞响应机制扩展；
- 4、企业级未授权访问漏洞防御实践；
- 5、浅谈企业SQL注入漏洞的危害与防御；
- 6、信息泄露之配置不当；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；



 jsrc_team

 京东安全应急响应中心

动动手指~关注下呗~😊