安全小课堂第八十八期【漏洞挖掘之服务器漏洞挖掘】

京东安全应急响应中心 3月19日

安全——毫无疑问是一个永恒的话题，尤其是随着互联网应用的普及，在越来越互联的今天，一台与互联网完全隔绝的服务器基本上也是“无用”的。如果说互联网是一个公共的空间，服务器则就是相应用户的自留地，它是用户自身应用与数据面向互联网的最终门户，也将是企业应用最关键的安全命脉。

JSRC**安全小课堂第八十八期，**邀请到**Rootsecurity**作为讲师就**漏洞挖掘之服务器漏洞挖掘**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

服务器的什么漏洞容易被攻击

京安小妹

Rootsecurity：

我个人挖掘比较多的首先是默认口令/弱口令，诸如一些基础设施的弱口令，服务器远程管理卡的弱口令之类的。举个服务器远程管理卡的例子（Dell，HP，IBM，HUAWEI）各大品牌都在列，比如Dell服务器的默认口令就是root:calvin，如果没有修改可以通过远程管理卡直接进入控制台获取服务器权限。弱口令就不多说了，目前大家能看到的一些僵尸主机会不断的在扫描公网的一些诸如ssh、ftp、rdp等服务，还有公开的字典，可以自行发挥，但成功率最高的无非就是admin:admin,admin:123456,test:test,test:123456等等。未授权，举个例子，redis未授权导致服务器沦陷，大致就两种思路，都是通过redis客户端来操作，一种是写一个公钥进去，本地就可以用私钥登录服务器了，另一种是写一个计划任务，无论计划任务的内容是什么，拿到服务器权限应该是没问题的了。权限绕过，举个例子，写一个好的爬虫，针对一些常见的url进行爬取，运气好的话，肯定会遇到没校验session或者http头部的，导致权限绕过可以查看一些比较敏感的信息，如果RP爆表还可能基于此找到危害更严重的漏洞哦。struts2这类的就不多说了，还有诸如weblogic，fastjson，jackson都出现过反序列化和命令执行。

讲师

服务器安全漏洞有哪些，都有什么危害

京安小妹

Rootsecurity：

类型上面已经举例了，我个人挖的比较多的其实还真就是弱口令。危害简单的说就是可以直接得到服务器的权限进而以此做为跳板继续渗透内网其他目标，可以辅助一些端口反弹，端口转发的小工具，效果更佳。

讲师

分享一些服务器安全漏洞挖据思路

京安小妹

Rootsecurity：

首先通过各种探测了解服务器的基本信息，比如探测目标操作系统、版本补丁、端口开放、服务运行状态情况等等。举一个windows环境下的例子：补丁没有及时更新，像去年5月份爆发的ms17-010,利用smb共享协议在内网快速传播。还有我以前经常利用的一个CVE-2016-0099（ms16-032），在windows 6.1+的内核上成功率在50%以上。

服务器安全漏洞检测工具分享

京安小妹

Rootsecurity：

我的工具基本上都是diy的，用别人的不多，电脑上可能开着的唯一一个第三方的工具就是Burpsuite了。举个例子，我比较依赖于python，像跑ssh弱口令，python的paramiko模块就搞定了，其他模块也有，比如libssh2之类的。

讲师

服务器漏洞的安全防范

京安小妹

Rootsecurity：
首先服务器一定要有一个安全基线，也就是要追溯问题的本质，为什么管理员可以设置弱口令，为什么ssh会对公网开放。其次是把补丁打全，特别是互联网已经公开了poc的漏洞。资产管理也是相对比较重要的，特别是对于京东这样的大公司，有时候离职没交接清楚，一些资产最终就不知道归属是谁了。像我们之前有一个外包的机器被人搞了，追溯原因就很简单，管理员设置了一个root:123456。所以要善用linux的一些自带的工具，比如audit和pam，避免麻烦。

：
讲师

白帽子提问:
有没有一些运维安全的思维导图可以参考学习学习
Rootsecurity:
https://github.com/phith0n/Mind-Map/blob/master/%E8%BF%90%E7%BB%B4%E5%AE%89%E5%85%A8.png
https://raw.githubusercontent.com/phith0n/Mind-Map/master/%E5%AE%89%E5%85%A8%E8%BF%90%E7%BB%B4%E8%84%91%E5%9B%BE.png

京东SRC三月境外游活动

正在火热进行中

挖洞即送出境游，参与即有钱+伴手礼！

详情请戳：

如果多9张机票，你会不会跟我一起走？

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，点击菜单栏进入“安全小课堂”即可浏览。

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