linux下破解SAM密码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_ti2020/619/2021_2022_linux_E4_B8_8B_E7_A0_c103_619613.htm 用linux启动，并挂载Windows的系统分区把c：\windows\system32\config\目录下的SAM和system复制出来 也可以用WINPE，DOS引导盘，都可以的，只要把SAM和system复制出来就行 开始破解： bkhive system keys 生成keys文件 samdump2 SAM keys gt. hashes john hashes 跑hashes 这样密码揪出来了 另外加上一些提示： 比如administrator密码是123456，那么他会在最底下这么显示 administrator ：123456：500：e263f50a6a506be3d494d3d62b4dc666：：：看起来有点像/etc/passwd的内容格式，如果当时没有看清楚密码就清屏了，或者linux认证，加入收藏！后来忘记已经破解了的密码，可以通过下面命令查看 john-1.7.2/run/john -show hashes有的时候密码处有可能会显示几个问号，如下 administrator：？？？456：500 ：e263f50a6a506be3d494d3d62b4dc666：：：这个时候可以通过 john-1.7.2/run/john -show hashes看看密码是否完整。 如果还是不完整，那么可能密码没有完全破解完毕，可以加restore参数从原来基础上继续破解 john-1.7.2/run/john restore hashes 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com