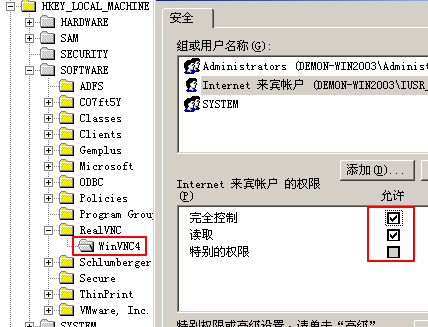
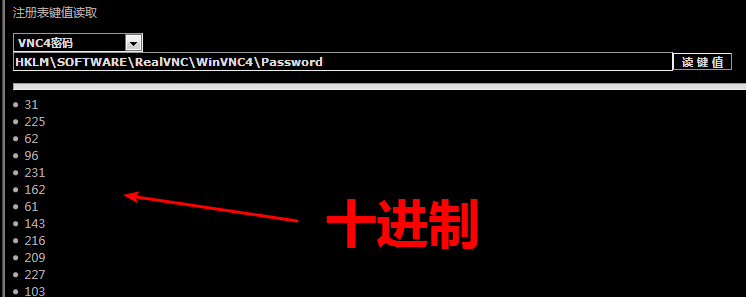
# vnc读取注册表提权

服务端配置连接密码，并且给来宾用户注册表可读权限

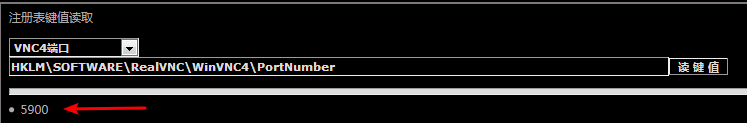




进入大马，在的读取注册表里，选择VNC4的键值，便可以读到密码（十进制）和端口

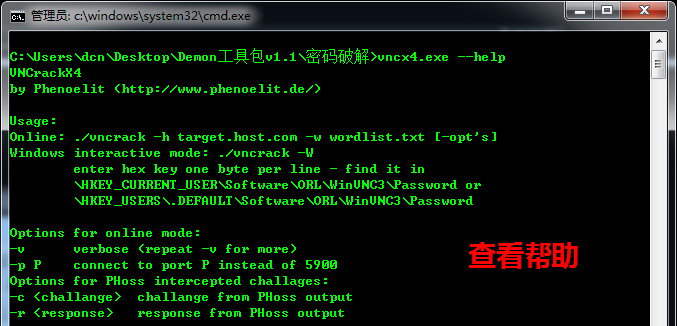


读取端口号

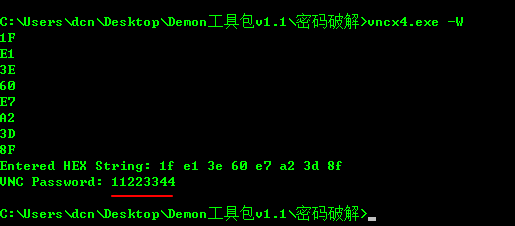


将密码：31 225 62 96 231 162 61 143 216 209 227 103 225 209 118 70 转成

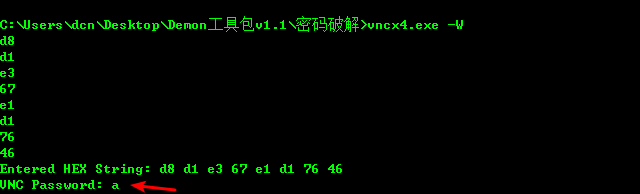
十六进：1F E1 3E 60 E7 A2 3D 8F D8 D1 E3 67 E1 D1 76 46



使用上图所示的VNC密码破解器破解密码，其中前64位为一组，前64位输入后得到的密码是前半部分的，如下图



输入后64位，将两部分的结果连接就是密码了

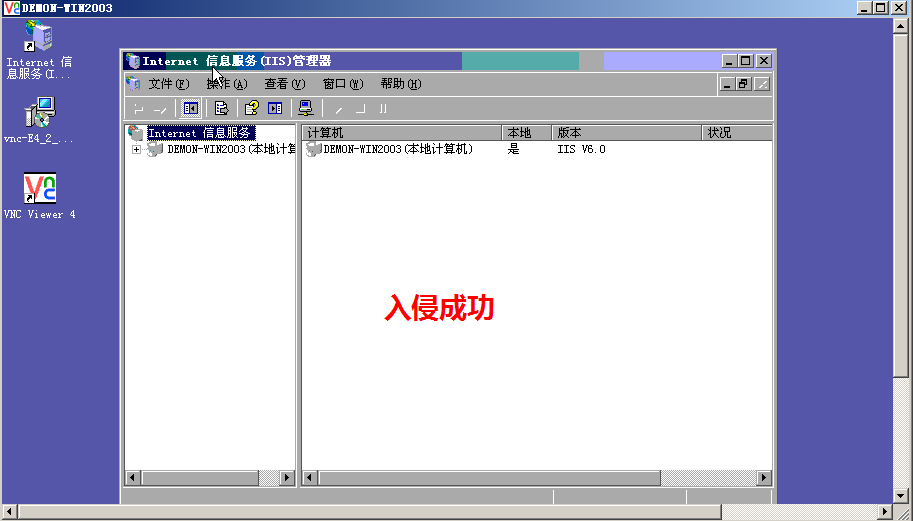


密码组合为： 11223344a

有了密码用vnc viewer 去连接即可

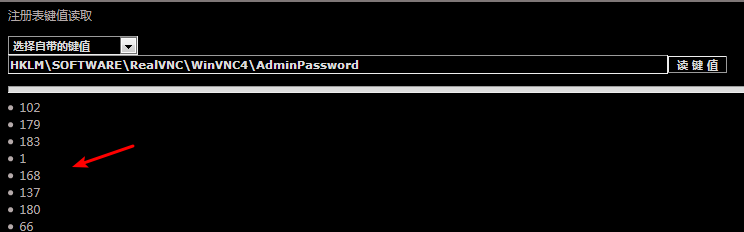






如果vnc启用的是admin用户，其密码的注册表键名为AdminPassword

HKLM\SOFTWARE\RealVNC\WinVNC4\AdminPassword



还有另外两个用户的密码注册表键名如下

HKLM\SOFTWARE\RealVNC\WinVNC4\InputOnlyPassword

HKLM\SOFTWARE\RealVNC\WinVNC4\ViewOnlyPassword

也可以通过读取UserPasswdVerifier键的值来判断认证模式

HKLM\SOFTWARE\RealVNC\WinVNC4\UserPasswdVerifier

None = 无密码认证

Vnc = VNCr认证

NtLogon = NT登录认证